DRAFT FSOR APPENDIX A – SUMMARIES AND RESPONSES TO 45 DAY COMMENTS

ARTICLE 1. GENERAL PROVISIONS – § 7001

Section of Regulation	Comment Numbers	Summary of Comments 45-Day Comment Period	Agency Response
7001(b)	1403	Comment suggests adding that the alternative opt-out link also refers to the ADMT opt-out as set forth in § 7221.	The Agency disagrees with this comment. The Pre-use Notice must include the opt-out link for requests to opt-out of ADMT. Comment's recommendation is less effective than the regulation, because it suggests that an opt-out link does not need to be included in the Pre-use Notice under § 7221(c)(1). A business must include an opt-out method with the Pre-use Notice to ensure that consumers can exercise their opt-out right when they are notified of a use of ADMT concerning them.
Previous 7001(c)	415, 716, 811, 844, 939, 977, 1308	Comment argues that the definition of "artificial intelligence" is overbroad and could include non-AI technologies that infer outputs from inputs, which lacks statutory basis and should not be included in § 7001(c). Comment states that this definition is unnecessary to implement the CCPA, as there is no statutory remand calling for its inclusion, and recommends its removal. In the alternative, comment suggests adopting a narrower definition that aligns with industry and scientific consensus, such as the NIST definition or the definition used in the California AI Transparency Act. Comment also suggests considering the OECD/EU AI Act definition, which defines AI as a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can	The Agency disagrees with this comment. The definition of artificial intelligence was informed by and harmonized with definitions in other frameworks, including NIST's. However, exercising its discretion, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time.

		influence physical or virtual environments. Comment argues that aligning with existing definitions, such as those in the NIST framework, AB 2885, or Government Code § 11546.45.5, would prevent regulatory fragmentation, simplify compliance for businesses, and avoid unnecessary confusion for customers. Comment further argues that AI is already covered under other governance frameworks and that the CPRA should focus on privacy concerns rather than broadly regulating AI. Accordingly, comment recommends removing "artificial intelligence" from the scope of ADMT definitions and obligations.	
Previous 7001(c)	449, 656, 946,1330, 1518, 1519, 1592, 1616, 1833, 1868, 1875, 1926	Comment argues that the definition of AI in § 7001(c) is overly broad, vague, overreaching, unnecessary, and not authorized by the statute. Comment asserts that the regulations inappropriately introduce AI as a separate regulatory category alongside ADMT, even though AI itself is broader and not explicitly covered by the CCPA, which creates confusion among businesses and consumers. Comment argues that the definition should be revised, limited to §7001(f)(1), or removed. Comment states that the definition goes beyond the CCPA's statutory mandate to issue regulations governing ADMT access and opt-out rights and could, based on some interpretations, include non-AI technologies that infer outputs from inputs. Comment argues that the plain text of the statute makes clear that the agency is only authorized to issue regulations that clarify how specific statutory provisions apply in the context of "businesses' use of automated decisionmaking technology" that is relevant to consumer privacy. The term ADMT is the closest CPRA gets to AI, and that term is undefined in CPRA, but is generally tied to	The Agency disagrees with this comment. The regulations, both as proposed and revised, are within the Agency's authority and further the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security to perform a thorough and independent annual cybersecurity audit. The CCPA also directs the Agency to require businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment and submit it to the Agency on a regular basis. (*See* Civ. Code § 1798.185(a)(14).) The CCPA further directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, it is required to issue regulations and impose certain requirements on these topics. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The

		profiling, which is limited to certain specific areas. The regulations introduce ambiguity by attempting to regulate AI broadly, including systems unrelated to personal information, which goes beyond the CCPA's privacy-focused remit. Comment expresses concern that the inclusion of AI in the rules is not limited to personal data processing and may encompass basic tools like spreadsheets and calculators. The definition introduces confusion by encompassing all systems that resemble or include AI (e.g., generative AI, AI models, AI systems), and therefore fails to calibrate requirements to the risks presented by different versions of AI technologies. Comment criticizes the definition for being vague, with overlapping language that creates significant interpretive challenges. Comment recommends that AI be more narrowly defined as systems that imitate intelligent human behavior and learn or adapt from data, or suggests using alternative language such as: "Artificial intelligence" means an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments." Comment suggests that the Agency use clearer and more direct language, avoiding anthropomorphizing AI by using terms like "infers" or pronouns like "it," which could undermine transparency and human oversight. Comment's recommended revisions draw from FTC language to enhance clarity and trustworthiness. Comment also explains that AI used in question writing, selection, and ordering in assessments is low-risk and does not involve personal information, and should not be treated as high risk under the Proposed	definition of artificial intelligence was clear and consistent with the OECD's definition. Nevertheless, exercising its discretion, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time.

		Regulations. Comment further argues that while AI used in personalized learning may involve personal data, it aligns with educational goals and is expected by individuals, and thus requires a nuanced risk assessment rather than a blanket "high risk" categorization. Comment states that the definition also diverges from international AI standards, creating regulatory inconsistencies. Comment argues that to the extent that a definition of AI is necessary for the limited purpose of giving meaning to how the Agency defines ADMT, the Agency should use the definition adopted in AB 2885.	
Previous 7001(c), 7001(e) [previously 7001(f)], 7001(fff)	1703	Comment argues that the Agency's regulations improperly extend beyond the agency's statutory authority by attempting to regulate AI, including its training, even when no automated decisions are made. Comment claims this overreach disrupts ongoing efforts by the California Legislature and Governor to create specialized, nuanced AI laws. Comment recommends removing "artificial intelligence" from the definitions and aligning any retained references with federal definitions. Comment recommends that the Agency should also consider deleting the reference to "artificial intelligence" from the definition of ADMT set forth in § 7001(f)(1); alternatively, to the extent the Agency does maintain AI as a subset of ADMT, it should define that term in alignment with federal law.	The Agency disagrees with this comment. The regulations, both as proposed and revised, are within the Agency's authority and further the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The CCPA also requires risk assessments for processing activities that present significant risk to consumers' privacy, regardless of whether they render a significant decision about a consumer. (*See* Civ. Code § 1798.185(a)(14)(B).) Nevertheless, exercising its discretion, the Agency removed references to artificial intelligence to further simplify implementation for businesses at this time. The proposed definition of artificial intelligence was clear and consistent with the OECD's definition. The Agency also modified the definition of 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 simplifying implementation for businesses at this time.

Previous 7001(c); 7001(e) [previously 7001(f)]	180	Comment suggests the deletion of § 7001(f)(1)-(4) and revise as suggested: "'Automated decisionmaking technology' or 'ADMT' means any solely automated processing of personal information to execute a decision which produces legal or similarly significant effects or replace human decisionmaking," or, in the alternative: "'Automated decisionmaking technology' or 'ADMT' means any solely automated processing of personal information to execute a decision or replace human decisionmaking." In addition, comment states that the defined term "artificial intelligence" should be deleted in § 7001(c).	The Agency disagrees with the comment. Nevertheless, the Agency revised the definition of 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 simplifying implementation for businesses. The Agency also deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time.
Previous 7001(c), previous 7150(b)(4), previous 7200(a)(3)	1018	Comment believes that the regulations extend risk assessments and other ADMT requirements to AI model training, not just deployment (§§ 7001(c), 7150(b)(4), 7200(a)(3)). This expansion exceeds the CPPA's statutory authority. Comment recommends that the Agency remove the definition of "training automated decisionmaking technology or artificial intelligence" and all related provisions. The CPPA should also remove the definition of "artificial intelligence" entirely, as this technology would already be covered by the definition of "automated decisionmaking technology," to the extent employed for such purposes.	The Agency disagrees with this comment. However, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time. The CCPA requires risk assessments for processing activities that present significant risk to consumers' privacy, regardless of whether they render a significant decision about a consumer. This includes training uses of consumers' personal information. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. With respect to other jurisdictions, the training threshold is consistent with the GDPR's framework for DPIAs. Further, AB 2013 is not a risk assessment law, it is a law that requires certain disclosures to the public. The risk assessment regulations are not about public disclosures of training data, but rather are focused on providing clarity about how to conduct a risk assessment for processing activities that present significant risk to consumers' privacy. Further, the Agency removed the training

			ADMT threshold from Article 11 to simplify implementation for businesses at this time.
Previous 7001(c), 7001(u) [previously 7001(w)], 7001(bb) [previously 7001(dd)]	1593	To the extent the regulations propose to add and define technical terms — such as "artificial intelligence," "multi-factor authentication," and "penetration testing" — comment recommends aligning its definitions with those drafted by national standards bodies, such as the National Institute of Standards and Technology (NIST), to prevent potential gaps and/or conflicts-of-law issues for businesses.	The Agency disagrees with this comment. Regarding "artificial intelligence," the definition was informed by and harmonized with definitions in other frameworks, including NIST's. However, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time. Regarding "multi-factor authentication," the definition is informed by and harmonizes with others' definitions of this term, such as those from the Federal Trade Commission (FTC), New York Department of Financial Services (NYDFS), and NIST (*See, e.g.*, SP 1800-12A.) Similarly, regarding "penetration testing," the definition is informed by other regulators' definitions and descriptions of this term, such as the FTC and NYDFS, and is aligned with NIST definitions. (*See*, e.g., NIST SP 800-53, Rev. 5.)
Previous 7001(c), 7001(e) [previously 7001(f)], previous 7001(ll)	1763	Comment argues that definitions such as "ADMT," "artificial intelligence," "significant decision," and "publicly accessible place" are overly broad or vague, leading to regulatory confusion and overreach. It calls for alignment with existing definitions in state and international frameworks such as the GDPR.	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT, including profiling. (*See* Civ. Code § 1798.185(a)(15).) The ADMT regulations, both as proposed and revised, are within the Agency's authority and further the intent and purpose of the CCPA. However, the Agency revised § 7200 to focus on the use of ADMT for significant decisions and revised the definition of ADMT to address the higher-risk use of ADMT without any human involvement. The Agency also revised the definition of significant decision to provide additional clarity and guidance for businesses, and to further simplify implementation for businesses

			at this time. As revised, the definition is consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. The proposed definition of artificial intelligence was clear and consistent with the OECD's definition. However, exercising its discretion, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time. The Agency also deleted the term "publicly accessible place."
7001(e) [previously 7001(f)]	81, 82, 83, 84, 547, 773, 774, 1043, 1078, 2051	Comment indicates that the rapid expansion of data-driven workplace technologies demands broad worker protections to address potential harms, including discrimination, privacy violations, and labor exploitation. The scope of ADMT must be comprehensive to ensure adequate safeguards. Comment advocates expanding the definition of ADMT to ensure broader coverage and accountability in employment-related AI systems. Comment supports the inclusion of worker data protections under the CCPA, emphasizing the need to regulate AI-driven scheduling, surveillance, and decision-making. Comment argues that ADMT provisions should cover employment decisions, allowing workers to challenge AI-driven discipline, scheduling, and performance tracking. Comment urges that full coverage and protection by the CCPA are critical first steps to ensure that California workers have the tools necessary to advocate for their rights in the 21st century data-driven workplace. Comment argues that the limited definition of "automated decision-making	The Agency agrees with this comment that it is necessary to protect consumers' privacy in the workplace and that businesses use automated tools in varying degrees. The regulations regarding risk assessments and ADMT provide several protections for workers. For example, businesses must conduct risk assessments prior to using ADMT to make a significant decision concerning them and prior to certain automated processing in the workplace. Businesses also must provide a Pre-use Notice prior to using ADMT to make a significant decision, and workers have opt-out and access rights to that use of ADMT. The Agency disagrees with this comment to the extent it recommends that the Agency broaden the definition of ADMT, and disagrees with the comment's point that attempting to create distinctions between levels of reliance is impractical. The Agency revised the definition of ADMT to focus on human involvement, to balance providing protections for consumers in higher-risk uses of ADMT with simplifying implementation for businesses at this time. The definition also aligns with

		tool" to "substantially facilitate" human decision-making may allow a company to claim the ADMT decision was simply advisory. Revising ADMT's definition from "facilitates" to "substantially facilitates" allows employers to evade oversight. Comment further asserts that this change creates loopholes where companies can self-certify out of compliance, making it difficult for workers and regulators to challenge unfair employment decisions. Comment states that employers use automated decision-making tools in varying degrees, from assisting human decision-making to fully automating employment-related choices. Comment argues that an employer could rely heavily on an automated system for promotions but avoid regulation by giving token weight to human reviews or establishing an internal policy that suggests (but does not ensure) human decision-making. This undermines transparency and allows employers to bypass ADMT rules. Attempting to create distinctions between these levels of reliance is impractical, and all forms of ADMT should be regulated. Comment urges a further strengthening of definitions of ADMT and stresses that businesses should not exploit ambiguity in definitions. While the Agency justifies including "substantially facilitate" in ADMT's definition to prevent harm when human decision-makers significantly rely on automated systems, comment believes that a stronger definition exists in the California State Administrative Manual; its broader definition better captures the impact of ADMTs and the full range of technologies that impact workers, and aligns with other regulatory efforts. If the Agency adopts the SAM definition, comment recommends clarifying that "material impact" has the	approaches taken in other jurisdictions, such as in the Colorado Privacy Act. The revised definition of ADMT provides a clear standard for what is in scope, and the regulations do not allow a business to self-certify that it is not using ADMT. As with other violations of the CCPA, the Agency has enforcement authority if a business is not complying with the law.

		same meaning as the definitions of "significant decision" and "profiling."	
7001(e) [previously 7001(f)]	158, 305, 317, 459, 463, 466, 469, 494, 534, 1045, 1093, 1118, 1133, 1895, 2038	Comment argues that the definition of ADMT in the regulations is overly broad, lacks clarity and fails to meet legal standards, and uses complex conditional language, making it very complicated and difficult for businesses — especially small businesses — to understand who needs to comply. The language could be interpreted to apply to nearly all business software, including common banking software, routine automation tools, and technologies that merely assist human decision-making, such as search results, binary screening questions, and HR platforms. This could hinder innovation and lead to unnecessary compliance costs, legal uncertainties, and challenges for digital businesses, without improving consumer privacy protections; it could also result in goods and services being less beneficial to consumers. Comment argues that the inclusion of general terms like "statistics" and "data processing techniques" further expands the scope unnecessarily, creating compliance challenges and potentially disrupting or unintentionally restricting internet advertising. This ambiguity fails the clarity requirement under Government Code § 11349(c), which mandates that regulations be written so those affected can easily understand them. The definition reaches far beyond AI or "automated" decisionmaking tools, potentially wiping out internet ads and burdening digital tools used in ways beneficial and expected by consumers. Comment urges the Agency to refine, simplify, or completely redraft the ADMT definition to focus only on high-risk AI tools that make independent decisions without human oversight and to ensure a balanced	The Agency disagrees with this comment. The ADMT definition is clear about what technologies are in scope and is not overly expansive. Exercising its discretion, the Agency revised the definition of ADMT to focus on the level of human involvement, which furthers both consumer privacy and simplifies implementation for businesses at this time.

DRAFT

		regulatory approach that safeguards rights while enabling innovation. Comment also suggests clarifying what qualifies as a "significant decision" impacting consumers and asks for a "carve-out"/"safe harbor" to reduce burdens of operating a simple AI chatbot, based on a commercial LLM. One comment recommends using the Colorado AI Act's definition of consequential decisions for clarity.	
7001(e) [previously 7001(f)]	181, 209, 225, 264, 336, 363, 392, 428, 487, 491, 517, 657, 658, 659, 660, 719, 752, 772, 786, 806, 812, 845, 883, 931, 947, 963, 1016, 1046, 1047, 1069, 1112, 1131, 1153, 1179, 1201, 1202, 1219, 1231, 1257, 1281,	Comment argues that the definition of ADMT is overly broad, vague, and expansive, capturing a wide range of routine and low-risk tools — such as spreadsheets, calculators, databases, basic analytics tools, and traditional computational software — that merely assist human decision-making rather than replace it. Comment emphasizes that the definition includes technologies not aligned with the term's focus on automation or AI and improperly encompasses tools like hiring assessments, performance feedback systems, and recommendation engines that do not make independent decisions. Comment highlights that terms like "substantially facilitate," "key factor," and "primary factor" are vague, subjective, and inconsistently applied, creating regulatory uncertainty, compliance challenges, and potential litigation. Comment warns that § 7001(f)(4)'s carve-outs are circular and confusing, with examples that could lead to inconsistent enforcement. Comment argues the definition diverges from global privacy frameworks like the GDPR, OECD, and California Assembly Bill 2885, and that the broad scope may stifle innovation, impose unnecessary compliance costs, and chill beneficial consumer-facing technologies like personalization and subscription optimization. Some recommend removing vague	The Agency disagrees with the comment. The Agency revised the definition of 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 simplifying implementation for businesses at this time. The revised definition of ADMT clearly defines "substantially replace human decisionmaking" and includes criteria to clarify the threshold of human involvement. Additionally, the listed technologies, such as spreadsheets, are now excluded from the definition of ADMT if they do not replace human decision-making.

	1290, 1319, 1654, 1659, 1706, 1751, 1855	terms, replacing "substantially" with clearer language like "materially" or the "substantial factor" test, and narrowing profiling to decisions with legal or significant effects. Others call for a risk-based or technology-agnostic approach that focuses only on high-risk or fully automated systems, and urge alignment with existing state privacy laws and definitions such as the State Administrative Manual (SAM). Several propose refining or redrafting the definition to ensure it excludes low-risk, human-assisted technologies and provides clear, enforceable thresholds that prevent loopholes while preserving consumer protections. Comment also supports carveouts for low-risk technologies but recommends additional categorical exemptions that are appropriately tailored to avoid unintended impacts to socially beneficial technologies and use cases.	
7001(e) [previously 7001(f)]	410, 572, 1027, 1173, 1177, 1190, 1305, 1371, 1594, 1927	Comment argues that the definition of ADMT is too broad, conflicts with the statute, and includes activities that do not independently or materially impact consumers, including any computerized assistance in decision-making even when humans remain in control. This will inhibit business practices that have been used for decades to more accurately and efficiently service customers and creates unnecessary ambiguity and compliance burdens. The Agency provides no evidence that technology-assisted human decisions increase privacy risks. The regulations are out of step with other privacy laws and should align with GDPR and other U.S. state privacy laws (e.g., Colorado and Connecticut), and the CPPA's role as a privacy regulator. Including technology that influences human decisions through "key" or "primary" factors lacks clarity. One comment suggests	The Agency disagrees with the comment. The comment does not support its argument that the definition of ADMT conflicts with the statute. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT but does not define ADMT. (Civ. Code § 1798.185(a)(15).) Regarding risks to consumers' privacy, the Agency provides ample evidence of the privacy risks associated with businesses' use of ADMT, including a lack of transparency for consumers to know when a business is using ADMT with respect to them, a lack of consumer control over how their personal information is processed using ADMT, and unlawful discrimination. However, the Agency modified the definition of 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

		defining the terms "key factor" and "primary factor" with examples or replacing them with clearer terms like "principal basis" or "controlling factor." Comment suggests limiting ADMT to when decisions are made solely by automation without human involvement and only include decisions that have "legal or similarly significant effects" on consumers, such as: financial/lending services, housing, insurance, education, criminal justice, employment, healthcare, or access to basic necessities. Another comment recommends revising the definition to mirror other commonly accepted ADMT definitions, directed to wholly automated (no direct human involvement) decisionmaking processes that use personal information to make decisions with legal or similarly significant effects on consumers. Comment further suggests that "legal or similarly significant effects" should be limited to effects on consumers, such as the provision of financial or lending services, housing, insurance, education enrollment or opportunities, criminal justice, employment opportunities, healthcare services, or access to basic necessities. This would avoid overregulating low-risk activities and unnecessarily burdening businesses and regulators. One comment suggests the definition should be revised to encompass only those technologies that (1) involve processing of personal information in a way that presents a significant privacy risk, (2) are not subject to human involvement, and (3) reach a significant decision to target obligations to activities most likely to present a heightened risk of harm to consumers. One comment suggests the following definition: "Automated decision making technology" means any solely automated technology that	simplifying implementation for businesses at this time. The revised definition of ADMT clearly defines "substantially replace human decisionmaking" and includes criteria to clarify the threshold of human involvement. Separately, with respect to the breadth of the ADMT regulations, the Agency revised § 7200 to focus on the use of ADMT for significant decisions to simplify implementation at this time. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. As revised, the regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. The definition of significant decision has also been revised to provide additional clarity and to further simplify implementation for businesses at this time.

		processes personal information and uses machine learning for the primary purpose of making a significant decision about a consumer without any human involvement." Another comment suggests similarly amending the definition: "ADMT means any solely automated technology that processes personal information and uses computation for the primary purpose of making a solely automated significant decision about a consumer to execute a decision, replace human decision-making, or substantially facilitate human decision-making" and would exclude "systems that perform procedural tasks, detect patterns, or provide insights for human decision-making without directly affecting the outcome of a decision." Another comment recommends deleting the definition of "automated decisionmaking" and using "human involved and human reviewed automated processing" from the Colorado Consumer Protection Act. Comment also suggests excepting online platforms that provide search results for a consumer to review. In addition, comment suggests deleting § 7001(f)(3), because profiling isn't decision making. Comment also suggests that the Agency remove the example from § 7001(f)(4) and specifically excluding any ADMT that includes a human in the decision-making tree from the application of the Proposed Regulations.	
7001(e) [previously 7001(f)]	884	Comment argues that including AI regulation in the ADMT exceeds the CPPA's legal authority, as the CCPA does not grant explicit jurisdiction over AI. The definition's lack of clarity could lead to unintended regulatory consequences, including limitations on routine business practices and potential harm to small businesses. Other states take a narrower approach,	The Agency disagrees with this comment. The regulations, both as proposed and revised, are within the Agency's authority and further the intent and purpose of the CCPA. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. Nevertheless, exercising its discretion, the Agency deleted the definition of artificial intelligence

		regulating only fully automated decisions that have significant legal effects.	as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time. The Agency also modified the definition of 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 simplifying implementation for businesses. Separately, the Agency revised the definition of significant decision, and revised § 7200 to focus on the use of ADMT for significant decisions to simplify implementation at this time. As revised, the regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope.
7001(e) [previously (f)]	1048	Comment suggests that exemptions for safety, security, and fraud prevention are essential but require clearer boundaries to prevent misuse. Similarly, safeguards for workplace and educational ADMT should balance consumer rights with operational needs. The rules should maintain focus on consumer personal information and exclude business characteristics, business data, and business products. Comment suggests the following definition of ADMT: "Automated decision making technology" means any solely automated technology that processes personal information and uses machine learning for the primary purpose of making a significant decision about a consumer without any human involvement."	The Agency disagrees with the comment. The Agency revised the definition of 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 simplifying implementation for businesses at this time. In addition, the regulations provide several protections for consumers. Businesses must conduct risk assessments prior to using ADMT to make a significant decision concerning them and prior to certain automated processing in the workplace, in educational programs, and based upon a consumer's presence in a sensitive location. Businesses must also provide a Pre-use Notice prior to using ADMT to make a significant decision. Further, consumers have opt-out and access rights to that use of ADMT. The regulations already focus on personal information as defined under the CCPA.

7001(e) [previously (f)]	1140	Comment argues that the proposed rule's broad definition of ADMT includes longstanding insurance industry tools such as risk-rating software, making compliance overly burdensome and disruptive to well-established practices.	The Agency disagrees with this comment. The CCPA includes data-level exemptions, including for information subject to GLBA and implementing regulations and for information governed by HIPAA; but it applies to "businesses," is intended to supplement federal and state law. (*See* Civ. Code §§ 1798.140(d), 1798.145(c)(1), (e), 1798.196.) The CCPA directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. In addition, the Agency revised the ADMT regulations to further simplify implementation for businesses at this time.
7001(e) [previously 7001(f)]	1331, 1332, 1517	Comment argues that the plain text of the statute requires that the regulations be limited to the processing of personal information by technology that both (1) is automated and (2) makes a decision. The draft regulations are overbroad on both points. Comment argues that where a human has the capability to overturn a decision, it is not automated. Also, technologies that substantially facilitate human decisionmaking exceeds the statute's direction to issue rules on automated decisionmaking because they are not making the decision themselves. Comment argues that the definition of ADMT ignores the fact that responsible human users of these ADMT systems are fully accountable for decisions made; computers, algorithms, and assessment tools do not know the bona fide applicable requirements surrounding the actual decision and, alone, cannot	The Agency disagrees with this comment. The regulations, both as proposed and revised, are within the Agency's authority and further the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT but does not define ADMT. (*See* Civ. Code § 1798.185(a).) The comment does not support its arguments that the definition of ADMT is overly broad, or that the definition of ADMT ignores human accountability. A human having the capability to overturn an automated decision does not render the automated decision no longer automated. However, exercising its discretion, the Agency modified the definition of 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 simplifying

		render decisions about an individual's suitability, qualifications, or competence. Instead, a true ADMT only informs the human decision-making process by providing evidence-based insights about related knowledge, skills, and abilities of the individual being evaluated. Comment recommends that the Agency revise the regulation to apply to only profiling involving solely automated technology for the primary purpose of making a significant decision about a consumer. Comment argues that the regulations are overbroad and could result in vague, arbitrary, and capricious regulations susceptible to administrative challenge. The regulations are circular and misleading. They claim not to include everyday technologies like a calculator or spellchecking, but only if they are not used for ADMT. Board Member Mactaggart recognized this concern. The ISOR also emphasizes that the regulations provide only an "illustrative" and "non-exhaustive" list.	implementation for businesses at this time. Further, the excepted technologies are now excluded from the definition of ADMT if they do not "replace" human decision-making.
7001(e) [previously 7001(f)]	1498	Comment disagrees with the revised definition of ADMT (Proposed Regulations December 2023 vs. current draft) for narrowing coverage by requiring a system to "substantially facilitate" decisionmaking rather than merely "facilitate" it. Comment is concerned that businesses will exploit this ambiguity, claim their systems don't substantially facilitate decisions, and thus avoid regulation and deny consumers opt-out rights. Comment recommends the Agency instead use the State Administrative Manual (SAM) definition of Automated Decision System for clarity and better protection.	The Agency disagrees with this comment. The Agency modified the definition of 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 simplifying implementation for businesses at this time. In addition, the regulations provide several protections for consumers. Businesses must conduct risk assessments prior to using ADMT to make a significant decision concerning a consumer and prior to certain automated processing in the workplace, in educational programs, and based upon a consumer's presence in a sensitive location. Businesses must also provide a Pre-use Notice prior to using ADMT to make a significant decision. Further,

			consumers have opt-out and access rights to that use of ADMT.
7001(e) [previously 7001(f)]	1528, 1529	Comment argues that the ADMT definition and examples conflict with existing exemptions in Cal. Civ. Code §§ 1798.145(d), (e). The use of ADMT in these scenarios is already governed by extensive federal rules. Comment argues that under the Proposed Regulations' definition of ADMT, automation tools would be considered ADMTs if the technology processes personal information and is used to facilitate human decision making, e.g., a "significant decisions." Further, the description of what is considered a "significant decision" includes instances that would generally be exempt from the CCPA because they involve personal information subject to the GLBA/CFIPA and FCRA. Such information should be exempted.	The Agency disagrees with this comment. The CCPA includes data-level exemptions for (1) information subject to GLBA and implementing regulations or the CFIPA and (2) the processing of personal information by certain entities, as long as the activity is regulated by the FCRA, and the processing is as authorized by the FCRA. (*See* Civ. Code §§ 1798.145(d), (e), 1798.196.) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; the CCPA's exemptions apply to the regulations. Nevertheless, the Agency modified the definition of 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 simplifying implementation for businesses at this time.
7001(e) [previously 7001(f)]	1543, 1617, 1647, 1651, 1652, 1848, 1854, 1949	Comment argues that the ADMT definition is vague, overly expansive, overlooks the vital role of human oversight in leveraging technology, and would wrongly classify basic Human Capital Management (HCM) software — like payroll systems or performance review tools — as ADMT, despite these tools not making autonomous decisions. Comment appreciates that the Agency narrowed the scope of the ADMT definition to those technologies that substantially facility a decision, but "substantially facilitates" is not clearly defined and should be amended to provide greater certainty to businesses and ensure that the CCPA takes a risk-focused approach to the use of ADMT. Terms like "key factor" and "primary factor" should be further defined through illustrative examples so businesses can reliably anticipate what technologies	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) However, the Agency modified the definition of 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 simplifying implementation for businesses at this time, including by providing flexibility for businesses to come into compliance. The revised definition of ADMT defines "substantially replace human decisionmaking" and includes criteria to clarify the threshold of human involvement. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The majority of the costs of the regulations fall

		and practices will fall within scope. One comment argues that including technology that "substantially facilitates human decision making" (i.e., "using the output of the technology as a key factor in a human's decision making," as when "a human reviewer uses [an output] as a primary factor to make a significant decision about them") will require an impossible line-drawing exercise (what is a "key/primary factor"? when are other factors considered by the reviewing human "key/primary" when they produce the same result recommended by the ADMT?), and will chill use of innovative technologies in California. An ADMT should not "substantially facilitate human decision-making" when it (i) performs a narrow procedural task, (ii) improves the result of a previously completed human activity, (iii) detects decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment without proper human review, or (iv) performs a preparatory task to an assessment relevant to a significant decision. Comment critiques the broad definition of ADMT and outlines specific compliance requirements that are especially burdensome for small businesses. These include risk assessments, consumer notices, opt-out mechanisms, and detailed reporting. Comment recommends limiting the definition to tools that actively replace or significantly alter human decision-making. Comment recommends aligning with narrower definitions used in jurisdictions like New York City and clarifying the term "substantially facilitate."	on larger businesses dealing with a large amount of personal information and with annual revenues that are greater than $28 million. Nevertheless, the Agency modified the regulations to significantly reduce the costs of the regulations on small businesses.

DRAFT

7001(e) [previously 7001(f)]	1679, 1965	The definition of ADMT should be strengthened. The Agency should adopt the State Administrative Manual's definition of ADMT because it is broader and more appropriate for regulating the commercial use of ADMTs. This will ensure that the definition will cover the most frequently used context of ADMT's for significant decisions. It covers the contexts in which ADMTs are most often used as part of significant decisions (i.e., to assist humans in making significant decisions). The Agency's ADMT definition risks creating a loophole for controllers to argue that they don't need to comply because they don't consider the ADMT to be "substantial" in facilitating a significant decision. The SAM definition explicitly includes uses of AI to produce a "score, classification, or recommendation." It is also already in use in CA so would better align the regulations with other areas of state policy on AI.	The Agency disagrees with this comment. However, the Agency modified the definition of 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 simplifying implementation for businesses at this time. In addition, the regulations provide several protections for workers. Businesses must conduct risk assessments prior to using ADMT to make a significant decision concerning them and prior to certain automated processing in the workplace. Businesses must also provide a Pre-use Notice prior to using ADMT to make a significant decision. Additionally, workers have opt-out and access rights with respect to that use of ADMT.
7001(e) [previously 7001(f)]	1876	Comment provides two revisions of the definition of ADMT, focusing on technology that replaces human decisionmaking and that would make the definition consistent with existing frameworks addressing the use of ADMTs. Comment suggests using California Gov. Code § 11546.45.5, and also suggests removing §§ 7001(f)(1), (2) and (4) entirely.	The Agency disagrees with this comment. However, the Agency revised the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision, and revised § 7200 to focus on the use of ADMT for significant decisions to simplify implementation at this time. As revised, the regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. The revisions include defining "substantially

			replace human decisionmaking" and including criteria to clarify the threshold of human involvement; deleting § 7001(f)(1) as unnecessary; and excluding the listed technologies in § 7001(e)(4), previously § 7001(f)(4), from the definition of ADMT if they do not "replace" human decision-making. The comment does not support that its proposed changes are more effective or appropriate than those proposed by the Agency.
7001(e) [previously 7001(f)]	1867	Comment recommends that the Agency narrow the ADMT definition and seek additional public comments. Comment suggests revising the definition as follows: "Automated decisionmaking technology" means any automated technology that processes personal information and uses computation for the primary purpose of making a solely automated significant decision about a consumer.	The Agency disagrees with this comment. However, the Agency modified the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision, and revised § 7200 to focus on the use of ADMT for significant decisions to simplify implementation at this time. The Agency has invited, received, and considered extensive public comments and feedback in both its preliminary rulemaking activities and the formal rulemaking process.
7001(e) [previously 7001(f)], 7001(ii) [previously 7001(kk)]	930	Comment argues that the proposed definitions of ADMT and "profiling" are overly broad and could negatively impact the growth of ADMT and the consumer experience. The definitions should be revised to focus on high-risk privacy concerns, ensure interoperability with other state laws, and avoid unnecessary restrictions on beneficial technologies. Specifically, § 7001(kk) expands "profiling" beyond existing privacy laws, causing inconsistencies and consumer confusion.	The Agency disagrees with this comment. The CCPA defines "profiling" and directs the Agency to further define it. (*See* Civ. Code §§ 1798.140(z), 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. In addition, the definition of "profiling" does not impose regulatory requirements upon businesses. The Agency modified the definition of 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 simplifying implementation for businesses at this time. Separately, with respect to the breadth of

			the ADMT regulations, the Agency revised § 7200 to focus on the use of ADMT for significant decisions to simplify implementation at this time. As revised, the regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. The definition of significant decision has also been revised to provide additional clarity and to further simplify implementation for businesses at this time.
7001(e), [previously 7001(f)], 7001(cc) [previously 7001(ee)], 7001(ii) [previously 7001(kk)]	1653	Comment urges the Agency to narrow the ADMT definition to exclude basic HCM tools and provide clearer guidance on what constitutes "profiling," "performance at work," and prohibited uses of general technologies. Comment recommends aligning with definitions like those used in New York City, limiting coverage to tools that play a "predominant or significant" role in decisionmaking.	The Agency disagrees with this comment. However, the Agency modified the definition of 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 simplifying implementation for businesses at this time. The revised definition of ADMT defines "substantially replace human decisionmaking" and includes criteria to clarify the threshold of human involvement. Separately, the Agency revised the definition of significant decision, and revised § 7200 to focus on the use of ADMT for significant decisions to simplify implementation at this time. As revised, the regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. The comment does not support that its proposed changes are more effective or appropriate than those proposed by the Agency. With respect to the definitions of "profiling" and "performance at work," the proposed regulations, including the definitions of those terms in §§ 7001(cc),

			(ii), are reasonably clear. The Agency believes that no further clarification is needed at this time.
7001(e) [previously 7001(f)], 7221	540	Comment argues that the definition of ADMT is overly broad and could apply to any technology used in human decision-making without assessing actual risks. In addition, managing opt-outs will be onerous, and take time and capital to develop. Small and local businesses lack those resources.	The Agency disagrees with this comment. However, the Agency revised the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision, and revised § 7200 to focus on the use of ADMT for significant decisions to simplify implementation at this time. As revised, the regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA, and modified the regulations to significantly reduce the costs of the regulations, including for small businesses.
7001(e)(1) [previously 7001(f)(2)], 7001(fff)	1297	Comment commends the Agency's broad definition of ADMT but recommends clarifications to prevent businesses from avoiding accountability. Comment also advocates for expanding the description of AI training processes.	With respect to the definition of ADMT, the Agency agrees with this comment to the extent that it supports preventing businesses from avoiding accountability. However, the Agency revised the definition of 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 simplifying implementation for businesses at this time. The listed technologies are now excluded from the definition of ADMT if they do not "replace" human decision-making. With respect to the definition of "train ADMT or AI," the Agency disagrees with this comment and modified the

			definition of "train" to align with revised risk-assessment requirements regarding training, and removed the definition's references to AI as unnecessary.
7001(e)(2) [previously 7001(f)(3)]	813	Comment affirms that profiling is a form of automated decision making, provided the profiling remains as defined in existing California privacy law.	The Agency agrees in part with this comment to the extent that it supports the regulations.
7001(e)(3) [previously 7001(f)(4)]	720	Comment states that the definition of "ADMT" purports to include an exception in 7001(f)(4), giving a long list of technologies that are not ADMTs. The problem, however, is that the exception is qualified: Those technologies are only excluded from the definition if they "do not execute a decision, replace human decision-making, or substantially facilitate human decisionmaking."	The Agency disagrees with this comment. However, the Agency modified the definition of 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 simplifying implementation for businesses at this time. Additionally, the listed technologies are now excluded from the definition of ADMT if they do not replace human decision-making.
7001(e)(3) [previously 7001(f)(4)]	814	Comment affirms the statement that these exclusions are not designed to allow for the circumvention of ADMT.	The Agency agrees with this comment to the extent that it supports the Agency's regulations.
7001(e)(3) [previously 7001(f)(4)]	1178	Comment claims that the rules include calculations, spreadsheets, and ride-sharing algorithms even with the exemption, which do not constitute true ADMT. Comment criticizes the inconsistent inclusion of some technologies while purportedly exempting others. Because the CCPA authorizes regulations only of automated decisionmaking, however, these regulations go well past their authorized scope.	The Agency disagrees with this comment. The ADMT regulations are within the Agency's authority and further the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT but does not define ADMT. (*See* Civ. Code § 1798.185(a).) However, exercising its discretion, the Agency revised the definition of 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 simplifying implementation for businesses at this time.

Previous 7001(g)	265, 305, 337, 411, 574, 589, 662, 885, 887, 1029, 1030, 1182, 1183, 1307, 1355, 1473, 1618, 1769, 1838, 1852, 1880	Comment argues that the regulations improperly expand the scope of behavioral advertising regulation beyond the CCPA's original intent, which was limited to "cross-context behavioral advertising." Comment objects to the removal of "cross-context" from the term and asserts that the definition now includes first-party advertising, which the CCPA explicitly excludes; comment argues that the existing CCPA framework exempts businesses' own marketing activities from opt-out requirements. This expanded definition exceeds the scope of the CPRA, conflicts with the CPRA's balance between consumer privacy and online business models and with other state privacy laws, imposes unauthorized requirements, and introduces a new opt-out right that is inconsistent with the statute. Comment argues that including ads based on both third-party and first-party data would have significant economic consequences, particularly for small and medium-sized businesses that rely on digital ad platforms. Comment further states that the definition imposes disclosure obligations, evaluations, and opt-out rights even for businesses using their own customer data for personalized advertising, despite Proposition 24's preamble and legislative history confirming that it was meant to regulate third-party advertising, not a business's own use of customer data. Comment argues this redefinition of "behavioral advertising" could stifle innovation, limit consumer choice, harm businesses, create regulatory confusion, and burden protected First Amendment activity, unconstitutionally restricting first-party advertising. Comment urges the Agency to strike the definition of "behavioral advertising" entirely or revise it to align with the CCPA's existing definition of "cross-context	The Agency disagrees with this comment. The regulations, both as proposed and revised, are within the Agency's authority, and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(14)-(15).) In addition, the regulations as initially proposed did not contradict the existing CCPA opt-out framework, and the Agency does not believe that the definition or the associated requirements would have violated the First Amendment or conflicted with other state privacy laws. However, the Agency revised the regulations to remove the definition of behavioral advertising, and to remove the profiling for behavioral advertising thresholds from Articles 10 and 11, to simplify implementation for businesses at this time.

		behavioral advertising" in § 1798.140(k). Comment points out that conflating behavioral advertising with profiling under ADMT is inappropriate, since ad-delivery systems do not make decisions about individuals, and regulating them as ADMT offers no meaningful privacy benefit. Comment also warns that overlapping opt-out rights, which cover both ADMT for behavioral advertising and sharing for cross-context behavioral advertising, are duplicative, risk confusing consumers, and create compliance uncertainty. Comment argues that including behavioral advertising within the definition of ADMT is overly broad and misaligned with both consumer expectations and the intent of the CCPA. Comment stresses that first-party personalization provides real consumer benefits, poses low privacy risks, and should not be subject to ADMT regulations. Comment recommends eliminating all references to first-party behavioral advertising.	
Previous 7001(g)	213, 432, 815, 949, 953, 954, 1017, 1117, 1155, 1302, 1322, 1853, 1869	Comment argues that the regulations define "behavioral advertising" in an overly broad manner that likely exceeds the Agency's authority. The definition includes any targeting based on consumer activity, both across and within a business's own services, expanding beyond cross-context behavioral advertising (CCBA) to include first-party advertising on a business's own websites and apps. Comment states that the definition should not include personalization using data collected within the business's own services (commonly called "first-party data"), as this contradicts established regulatory norms and is inconsistent with the privacy laws of other states, which typically limit consumer opt-out rights to CCBA. Comment asserts that the proposed regulations could unintentionally restrict useful	The Agency agrees with this comment's points that the definition of behavioral advertising was more expansive than cross-context behavioral advertising and that the opt-out from a business's use of ADMT for profiling for behavioral advertising would have been more expansive than the opt-out from cross-context behavioral advertising. The regulations, both as proposed and revised, are within the Agency's authority and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(14)-(15).) Nevertheless, the Agency revised the regulations to remove the definition of behavioral advertising, and to remove the profiling for behavioral advertising thresholds from Articles 10 and 11, to simplify implementation for businesses at this time.

		website personalization, prevent businesses from displaying relevant product recommendations based on user interactions on their own platforms, and unnecessarily restrict businesses' ability to engage in first-party advertising, making it difficult to send personalized promotions to existing customers despite this being a common and consumer-friendly practice. This could particularly impact small businesses, minority entrepreneurs, and emerging brands with limited ad budgets, stifling competition and increasing consumer prices. Comment argues that the proposed regulations extend opt-out rights for "profiling for behavioral advertising" beyond the existing CCPA 1798.140(k) provision for CCBA by including first-party targeted advertising (§§ 7001(g), 7150(b)(3)(B)(iii), 7200(a)(1)(A)(ii), 7221(b)(6).) Implementing the required opt-out systems would be technically infeasible for many businesses, especially small ones. Comment recommends removing behavioral advertising provisions entirely, as they are mismatched with the concept of automated decisionmaking and likely to lead to increased consumer confusion over the exercise of privacy rights. Comment recommends at least removing "profiling for behavioral advertising" from the activities that give rise to an ADMT opt out right, due to tension with the text of the CCPA and the potential to undermine rather than advance consumer privacy interests. Another comment recommends revising the definition of behavioral advertising to exempt first-party advertising, and to clarify its scope, noting that the current definition includes low-risk activities and imposes significant additional compliance burdens without corresponding consumer benefits. Comment	

		also argues that the regulations unnecessarily group CCBA under the broader term "behavioral advertising," even though CCBA is already clearly defined and regulated under the CCPA. Comment asserts that the proposed regulations introduce overlapping and redundant opt-out mechanisms for CCBA, which is already subject to clear opt-out rights under the CCPA. Adding an opt-out under behavioral advertising would be duplicative, may confuse or mislead consumers, and create unnecessary compliance burdens for businesses. Comment recommends removing CCBA from the definition of "behavioral advertising" and making reference to the CCPA definition in §1798.140(k).	
Previous 7001(g)	775	Comment agrees that the definition of "behavioral advertising" in the regulations is appropriately scoped, as it includes cross-contextual advertising while excluding non-personalized advertising, aligning with the CCPA. This ensures businesses can still use advertising methods that do not rely on consumer profiling while preventing the exploitation of personal data.	The Agency notes this comment of support. However, the Agency revised the regulations to remove the definition of behavioral advertising, and to remove the profiling for behavioral advertising thresholds from Articles 10 and 11, to simplify implementation for businesses at this time.
Previous 7001(g)	789	Comment is concerned that adding the activity of a user within a business' own websites/services as part of the behavioral advertising definition would make it so that contracting with an entity to provide behavioral advertising based on a user's activity across internal platforms/websites would make the entity a "third party" and not a "service provider," under CCPA. We suggest that this definition be deleted. Instead, the definition of "cross-context behavioral advertising" of the CCPA should be used.	The Agency disagrees with this comment. However, the Agency revised the regulations to remove the definition of behavioral advertising to simplify implementation for businesses at this time. To the extent the comment objects to the CCPA's requirements with respect cross-context behavioral advertising, the comment is not on the rulemaking action.

Previous 7001(g)	964	Comment argues that the Agency's expansion of "behavioral advertising" beyond cross-context behavioral advertising (CCBA) is beneficial. It addresses harmful profiling-based targeted advertising, which has been linked to predatory and exploitative practices.	The Agency agrees with this comment to the extent that it suggests that addressing behavioral advertising would have provided further privacy protections for consumers. The regulations, both as proposed and revised, are within the Agency's authority and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(14)-(15).) However, the Agency revised the regulations to remove the definition of behavioral advertising, and to remove the profiling for behavioral advertising thresholds from Articles 10 and 11, to simplify implementation for businesses at this time.
Previous 7001(g), previous 7200(a)(2)(C), previous 7221(b)(6)	1293	Comment supports stronger opt-out rules for behavioral advertising due to its potential harm to children, including excessive engagement and exposure to extreme content. Comment argues that behavioral ads contribute to pervasive tracking and profiling, making stronger privacy protections necessary.	The Agency agrees with this comment to the extent that it suggests that providing an opt-out from profiling for behavioral advertising would have provided further privacy protections for consumers. The regulations, both as proposed and revised, are within the Agency's authority and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(14)-(15).) However, the Agency revised the regulations to remove the definition of behavioral advertising, and to remove the profiling for behavioral advertising thresholds from Articles 10 and 11, to simplify implementation for businesses at this time.
Previous 7001(g), previous 7150(b)(3)(B)(iii), previous 7200(a)(2)(C)	1710, 1711	Comment argues that the regulations treat first-party advertising as though it poses the same or greater risk than third-party advertising or data sales, which contradicts the intent of the CCPA/CPRA. This treatment could overwhelm consumers with unnecessary and confusing notices, especially compared to the lighter requirements placed on more invasive practices like data sales. Required pre-use notices for first-party advertising are overly intrusive and not aligned with actual risk, possibly leading to	The Agency disagrees with this comment. The regulations, both as proposed and revised, are within the Agency's authority and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(14)-(15).) However, the Agency revised the regulations to remove the definition of behavioral advertising, and to remove the profiling for behavioral advertising thresholds from Articles 10 and 11, to simplify implementation for businesses at this time.

		consumer confusion and unintended consequences such as opting for less privacy-friendly third-party ads. This treatment of first-party advertising would also be at odds with the text and structure of the CCPA, both when enacted by the Legislature and when amended by the CPRA. Comment suggests removing the concept of "behavioral advertising" from the Proposed Regulations by striking "profiling a consumer for behavioral advertising" as a trigger for ADMT or risk assessments by striking § 7200(a)(2)(C) and § 7150(b)(3)(B)(iii) and in their entirety, and deleting the definition of "behavioral advertising."	
Previous 7001(g), 7150(b)(3)	1831	Comment urges the Agency to ensure that the regulations reflect the limited scope of the statute. For example, the CPPA should not require risk assessments for (i) profiling a consumer for behavioral advertising or (ii) processing personal information to train ADMT or artificial intelligence. Comment argues that behavioral advertising based on first-party data does not pose significant risk and therefore should not trigger a risk assessment. Comment also argues that many AI uses do not pose significant privacy or security risks. Thus, the rules should identify specific criteria similar to those described in the prior section on cybersecurity audits to consider whether the processing activity's nature and sensitivity level poses a significant risk to consumers' privacy and security.	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(14)-(15).) Nevertheless, the Agency revised the regulations to remove the profiling for behavioral advertising thresholds from Articles 10 and 11, and to remove the training threshold from Article 11, to simplify implementation for businesses at this time. The risk assessment regulations require a risk assessment for certain training uses of consumers' personal information, because these uses present significant risk to consumers' privacy.
7001(j) [previously 7001(*l*)], 7001(k)	1695	Comment states that the cybersecurity audit definitions provide clarity to covered businesses and customers. Comment supports the definitions of "cybersecurity audit" and "cybersecurity program."	The Agency agrees with this comment to the extent that it supports the regulations and notes comment's support.

[previously 7001(m)]		They make the regulations more readable and understandable.	
7001(j) [previously 7001(*l*)]	1822	Comment suggests revising § 7001(*l*) as follows: "Cybersecurity audit" means audit that every business whom is processing consumers' personal information as set forth in § 7120, subsection (b), is required to complete.	The Agency disagrees with this comment. The comment's suggestion does not substantively change the definition and is not more effective or appropriate than the Agency's regulation.
Previous 7001(n)	816	Comment recommends avoiding a definition of "deepfake" because a definition and specific term is not required. The law should care about and require: Any content (e.g., audio, video, text) that is generated or changed, manipulated, or altered from its original state must include one or more of the following: A. Overlays an indelible, readable, and accessible watermark associated with the generation or party authoring the change, manipulation, or alteration; B. Marks the content in an indelible, readable, and accessible format as "created", "manufactured", "generated", or "altered" by the party generating or authoring the change, manipulation, or alteration; C. Establish the technical metadata in the content that distinguishes the content from the original content metadata. If it becomes necessary to define "deepfakes," comment suggests reverting the definition used in Sec. 20512(d) of CA AB-2655, signed by Gov. Newsom 9/17/2024, which defines "deepfake" as: "means audio or visual media that is digitally created or modified such that it would falsely appear to a reasonable person to be an authentic record of the actual speech or conduct of the individual depicted in the media."	The Agency disagrees with this comment. Comment's recommendation is less effective than the Agency's definition, which provided a clear definition of the term "deepfake" for purposes of conducting a risk assessment or providing an opt-out of ADMT. However, the Agency modified the regulations to remove the term "deepfake" and the corresponding thresholds explicitly referencing that term, to simplify implementation for businesses at this time.

Previous 7001(n)	978	Comment suggests that the definition of "deepfake" should explicitly reference AI and similar technologies to ensure it remains relevant as synthetic media evolves. Without this revision, enforcement challenges and First Amendment concerns could arise. Comment recommends adding "created using artificial intelligence or similar technologies" to the definition.	The Agency disagrees with this comment. Comment's recommendation is less effective than the Agency's proposed definition, which provides a clear definition of the term "deepfake" for purposes of conducting a risk assessment or providing an opt-out of ADMT. In addition, the Agency does not believe that the definition or the associated requirements would have violated the First Amendment. However, the Agency revised the regulations to remove the term "deepfake" and the corresponding thresholds explicitly referencing that term, to simplify implementation for businesses at this time.
Previous 7001(n)	1404, 1832	Comment suggests that the Agency delete the "deepfake" definition. Comment argues that that regulating deepfakes is beyond the Agency's rulemaking authority and is best left to the Legislature to address.	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(14)-(15).) However, the Agency revised the regulations to remove the term "deepfake" and the corresponding thresholds explicitly referencing that term, to simplify implementation for businesses at this time.
7001(t) [previously 7001(v)]	846	Comment believes that proposed text's definition of "information system" deviates from the GLBA Safeguards' and NY DFS's definitions by failing to specify electronic information. Comment recommends adding "a discrete set of electronic information," to add clarity and promote consistency among relevant definitions.	The Agency disagrees with this comment. The definition covers electronic information resources and is informed by, and is aligned with, others' definitions of this term, including the National Institute of Standards and Technology and the New York State Department of Financial Services. The definition is similarly aligned with the definition in the GLBA Safeguards Rule. However, the Agency revised the definition of "information system" to focus on "personal information."

7001(t) [previously 7001(v)]	1405	Comment recommends that the Agency add "personal" to the definition of "information system."	The Agency agrees with this comment in part and revised the definition of "information system" to focus on "personal information."
7001(t) [previously 7001(v)]	1812	Comment urges the Agency to consider expanding the definition of "information system" to include services available over an internet connection. This clarifies to the reader that services available over the internet are included in the definition of an information system.	The Agency disagrees with this comment. However, the Agency revised the definition of "information system" to clarify that the information system for which the business is responsible includes the use of a service provider's or contractor's resources.
7001(u) [previously 7001(w)]	847	Comment supports this definition and standardization of terms as it aligns with the definition in the GLBA and NY DFS. Consistency in terminology supports the CPPA's stated goal of simplifying compliance for businesses who must comply with multiple laws and avoiding unnecessary confusion.	The Agency agrees with this comment to the extent that it supports the Agency's regulations and notes comment's support.
7001(v) [previously 7001(x)]	900	Comment asserts that the revised text creates confusion regarding the scope of the CCPA's applicability to nonprofits. The Agency should take steps to align the regulations with the text of the statute by including text that appropriately limits the CCPA's applicability to nonprofits.	The Agency disagrees with this comment. The revision does align the regulation with the text of the CCPA. The CCPA defines "business" to include non-profits that control or are controlled by a business that share common branding with the business and with whom the business shares consumer personal information. (*See* Civ. Code § 1798.140(d)(2).)
7001(bb) [previously (dd)]	848	Comment supports this definition and standardization of terms as it aligns with the GLBA and NY DFS.	The Agency agrees with this comment and notes comment's support.
7001(bb) [previously 7001(dd)]	580, 718, 1823	Comment recommends modifying the definition of "penetration testing" to align with the NIST framework, arguing that the current language could create conflicts with federal cybersecurity standards or create a gap. It should be amended to align with the most current NIST definition. One comment suggests revising 7001(dd) as follows: "Penetration testing"	The Agency disagrees with this comment. The NIST Cybersecurity Framework does not define "penetration testing," while the definition in the regulation is informed by other regulators' definitions and descriptions of this term, such as the Federal Trade Commission and the New York Department of Financial Services. (*See* 16 C.F.R. § 314.2(n); N.Y. Comp. Codes R.

		means authorized testing of an information system by attempting to circumvent or defeat its security features.	& Regs. tit. 23, § 500.01(*l*).) The definition is also aligned with NIST definitions in other NIST publications. (*See* NIST SP 800-53, Rev. 5.) The comment's suggested revision is not more effective or appropriate than the Agency's regulation.
7001(cc) [previously 7001(ee)]	979	Comment suggests that the definition of "performance at work" should allow businesses to track company assets for security purposes without being overly restrictive. The proposed revisions clarify that businesses can monitor device location solely to protect confidential information. Comment recommends modifying the definition with the phrase: "a consumer's location when off-duty or on breaks unless used solely to track the location of business assets (e.g., business mobile devices and laptops) to protect the security of the business's information systems or to prevent the disclosure of confidential information."	The Agency disagrees with this comment. The Agency has determined that a device's location is not relevant to an employee's performance at work and has therefore not included it in the definition of "performance at work."
7001(cc) [previously 7001(ee)]	1406	Comment requests that the Agency delete "performance at work" definition as unnecessary because definition of "profiling" should be changed to not include employment related activities.	The Agency disagrees with this comment. The CCPA applies to consumers, including in their capacity as employees, applicants, and independent contractors; and "profiling" includes "performance at work." (*See* Civ. Code § 1798.125(a)(1)(E); 1798.140(z).) Defining "performance at work" is necessary to clarify what that term does and does not include. Under certain circumstances, a business must conduct a risk-assessment when it uses automated processing to infer or extrapolate a consumer's performance at work. (*See* §§ 7150 (b)(4)-(5).) In addition, exceptions may apply to a business's requirement to provide an opt-out from ADMT where the business uses the ADMT solely

			to assess the consumer's performance at work. (*See* §§ 7221(b)(2)(A), (b)(3)(A).)
7001(cc) [previously 7001(ee)], 7152(a)(5)	965	Comment suggests that the definition of "performance at work" should be broadened to protect employees from overreaching employer surveillance, particularly regarding union-related activities, personal time, and off-duty behavior, as well as associations, expressions, relationships, and constitutional harms. The December 2023 draft's language regarding workplace harms should be restored.	The Agency disagrees with this comment. The definition of "performance at work" already clarifies that a consumer's union membership or interest in union membership, their interest in seeking other employment opportunities, their location outside of their job duties, or certain uses of their personal accounts are not "performance at work." Businesses cannot, therefore, qualify for the exceptions that may apply to providing consumers with an opt-out from ADMT when the business uses ADMT solely to assess the consumer's performance at work. (*See* §§ 7221(b)(2)(A), (b)(3)(A).) With regard to broader protections for employees, the regulations require businesses to conduct a risk-assessment when they use automated processing to infer or extrapolate a consumer's performance at work under certain circumstances. (*See* §§ 7150 (b)(4)–(5).) The regulations provide clarity about the negative impacts to consumers' privacy that businesses may consider. (*See* § 7152(a)(5).) Because the regulations are intended to apply to a variety of industries and contexts, the negative impacts listed are non-exhaustive. Businesses may consider other negative impacts. The Agency does not believe additional examples are necessary at this time. Further, with respect to the December 2023 language, the Agency removed this language to further simplify implementation for businesses at this time, but businesses may still consider these types of harms.

DRAFT

7001(dd) [previously 7001(ff)]	1407	Comment suggests that the Agency delete "performance in an educational program" definition as unnecessary because of suggested changes to § 7221 on requests to opt-out of ADMT.	The Agency disagrees with this comment. Defining "performance in an educational program" is necessary to clarify what that term does and does not include. Under certain circumstances, a business must conduct a risk-assessment when it uses automated processing to infer or extrapolate a consumer's performance in an educational program. (*See* §§ 7150 (b)(4)-(5).) In addition, exceptions may apply to a business's requirement to provide an opt-out from ADMT where the business uses the ADMT solely to assess the consumer's performance in an educational program. (*See* §§ 7221(b)(2)(A), (b)(3)(A).)
7001(ee) [previously 7001(gg)]	266	Comment states that the definition of "physical or biological identification or profiling" information in the proposed regulations is overly broad, as it could encompass virtually any use of data related to the body, even if the data is not collected directly from the body and is instead observed and manually documented.	The Agency agrees with this comment in part and revised § 7001(ee), previously § 7001(gg), to clarify that this term means "automated measurements or analysis" and does not include processing physical or biological characteristics that do not identify, and cannot reasonably be linked with, a particular consumer.
7001(ee) [previously 7001(gg)]	575	Comment argues that the definition of "physical or biological identification or profiling" assumes all such identification is done without consent, which is not accurate. Comment proposes a revision that excludes cases where businesses notify consumers in advance and clarify that processing which does not identify individuals should not fall under this category.	The Agency disagrees with this comment. Nevertheless, the Agency revised § 7001(ee), previously § 7001(gg), to clarify that this term means "automated measurements or analysis" and does not include processing physical or biological characteristics that do not identify, and cannot reasonably be linked with, a particular consumer. Regarding consent, the definition of the term is separate from whether a consumer consents, and the Agency disagrees with excluding from the definition instances in which a business notifies consumers of its planned use of physical or biological identification or profiling.

7001(ee) [previously 7001(gg)]	940	Comment argues that the definition of "physical or biological identification or profiling" in § 7001(gg) should exclude photographs and videos, as many other states already make this distinction.	The Agency disagrees with this comment. Other states do not define "physical or biological identification or profiling"; they define "biometric data." In California, the CCPA defines "biometric information," and the Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The Agency revised § 7001(ee), previously § 7001(gg), to clarify that this term does not include processing physical or biological characteristics that do not identify, and cannot reasonably be linked with, a particular consumer; and to clarify that it includes automated measurements or analysis.
7001(ee) [previously 7001(gg)]	980	Comment recommends that the definition of biometric information should explicitly reference California Civil Code § 1798.140(c) for consistency with existing privacy laws. Comment suggests adding a phrase: "as defined in section 1798.140(c)."	The Agency disagrees with this comment. The regulations do not define "biometric information"; they define "physical or biological identification or profiling." The existing regulations already make clear that the definitions set forth in Civil Code section 1798.140 apply. (*See* § 7001.) The regulation is reasonably clear based on the plain meaning of the words. The Agency believes that no further clarification is needed at this time. However, the Agency revised § 7001(ee), previously § 7001(gg), to clarify that this term does not include processing physical or biological characteristics that do not identify, and cannot reasonably be linked with, a particular consumer; and to clarify that it includes automated measurements or analysis.
7001(ee) [previously 7001(gg)], 7201	1184	Comment asserts that the regulations impose new obligations on businesses using physical or biological identification, such as requiring evaluations, anti-discrimination safeguards, and staff training. These exceed the CPPA's authority, which is limited to access and opt-out rights for automated decision-	The Agency disagrees with this comment. The regulations, both as proposed and revised, are within the Agency's authority and further the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ.

		making. Comment argues that identification is not profiling.	Code §§ 1798.185(a)(15), (b).) However, exercising its discretion, the Agency revised the ADMT requirements to focus on the use of ADMT for significant decisions. The Agency also deleted § 7201, which imposed requirements for physical or biological identification or profiling, to simplify implementation at this time; and the ADMT regulations no longer reference "physical or biological identification or profiling."
7001(ee) [previously 7001(gg)]	1186	Comment asserts that at a minimum, "identification" and "identifying" should be removed from the definition.	The Agency disagrees with this comment. However, the Agency revised § 7001(ee), previously § 7001(gg), to clarify that this term means automated measurements or analysis and does not include processing physical or biological characteristics that do not identify, and cannot reasonably be linked with, a particular consumer. In addition, the Agency revised the ADMT requirements to focus on the use of ADMT for significant decisions. The Agency also deleted § 7201, which imposed requirements for physical or biological identification or profiling, to simplify implementation at this time; and the ADMT regulations no longer reference "physical or biological identification or profiling."
7001(ee) [previously 7001(gg)]	1408	Comment recommends that the Agency delete "physical or biological identification of profiling."	The Agency disagrees with this comment. However, the Agency revised § 7001(ee), previously § 7001(gg), to clarify that this term means "automated measurements or analysis" and does not include processing physical or biological characteristics that do not identify, and cannot reasonably be linked with, a particular consumer.
7001(ee) [previously 7001(gg)]	1717	Comment suggests removing "or profiling" in the section, and deleting the sentence "vocal intonation,	The Agency disagrees with this comment, because removing those terms would reduce privacy protections for consumers, and retaining them is necessary to clarify what constitutes "physical or

		facial expression, and gesture (e.g., to identify or infer emotion)."	biological identification or profiling" and what is therefore in scope of the revised risk-assessment threshold criteria in §§ 7150(b)(4) and (6). However, the Agency revised § 7001(ee), previously § 7001(gg), to clarify that this definition means automated measurements or analysis and does not include processing physical or biological characteristics that do not identify, and cannot reasonably be linked with, a particular consumer.
7001(hh) [previously 7001(jj)]	849	Comment believes that this definition aligns with the definition from the NY DFS Cybersecurity Regulations, and supports consistency in terminology.	The Agency agrees with this comment to the extent that it supports the regulations and notes comment's support.
7001(ii), [previously 7001(kk)]	576	Comment raises concerns that the profiling definition is excessively broad and could cover non-sensitive activities like predicting pedestrian movement. Comment proposes limiting the definition to significant predictions about intelligence, ability, economic status, or health rather than general behavioral observations.	The Agency disagrees with this comment. The CCPA defines "profiling" and directs the Agency to further define it. (*See* Civ. Code §§ 1798.140(z), 1798.185(a)(15).) The CCPA's definition of profiling includes predictions concerning a natural person's behavior, location, or movements. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
7001(ii), [previously 7001(kk)]	663	Comment states that the profiling definition is too broad, jeopardizing consumer safety, security, and business operations. The scope should be narrowed to exclude security and fraud-prevention technologies and focus on legally significant decisions. The definition should be aligned with frameworks in Colorado and Virginia, which only regulate profiling when it leads to legally significant outcomes. The "security, fraud prevention, and safety exception" is too narrow and should be broadened to ensure the continued operation of protective technologies.	The Agency disagrees with this comment. The CCPA defines "profiling" and directs the Agency to further define it. (*See* Civ. Code §§ 1798.140(z), 1798.185(a)(15).) The CCPA's definition of profiling includes predictions concerning a natural person's behavior, location, or movements. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. In addition, the definition of "profiling" does not impose regulatory requirements upon businesses. The Agency also modified the definition of 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 simplifying implementation for businesses at this time. Separately,

			the Agency revised the definition of significant decision and § 7200, to focus on the use of ADMT for significant decisions to simplify implementation at this time. As revised, the regulations are consistent with approaches taken in other jurisdictions, such as Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope.
7001(jj), [previously 7001(mm)]	1410	Comment recommends revising definition of "request to access ADMT" to add "personal information for…" and remove "with respect to the consumer."	The Agency disagrees with this comment. The CCPA is clear that the right to access is with respect to a business's use of ADMT, not just the use of personal information. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. In addition, the language regarding "with respect to the consumer" is necessary and clear regarding how the right to access ADMT works.
7001(kk) [previously 7001(nn)]	1411	Comment suggests that the Agency delete the "request to appeal ADMT" definition.	The Agency disagrees with this comment. This term is used within the regulations, and the definition is necessary to clarify what a "request to appeal ADMT" covers.
Previous 7001(ll)	267	Comment suggests that the California Penal Code already prohibits privacy invasions using cameras in areas where individuals have a reasonable expectation of privacy. The regulation should narrow its definition to focus on locations with heightened privacy or consumer protection concerns or those revealing sensitive information. Suggested examples include medical clinics, hospitals, airports, public Wi-Fi hotspots, workplaces, educational institutions, and government buildings.	The Agency agrees with this comment in part and deleted the term "publicly accessible place" and added the term "sensitive location," which includes healthcare facilities and educational institutions, among other sensitive locations. (*See* § 7001(aaa).)
Previous 7001(ll)	1409	Comment suggests revising definition of "publicly accessible place" to emphasize that it's a physical	The Agency agrees with this comment in part and deleted the term "publicly accessible place" and added

		place, removing several examples, and adding airports, educational institutions, and government buildings.	the term "sensitive location," which includes healthcare facilities and educational institutions, among other sensitive locations. (*See* § 7001(aaa).)
7001(ss) [previously 7001(vv)]	1412	Comment recommends that the Agency revise definition of "right to access ADMT" to add "personal information for…" and remove "with respect to the consumer."	The Agency disagrees with this comment. The CCPA is clear that the right to access is with respect to a business's use of ADMT, not just the use of personal information. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. In addition, the language regarding "with respect to the consumer" is necessary and clear regarding how the right to access ADMT works.
7001(xx) [previously 7001(aaa)]	1413	Comment asserts that the Agency should revise definition of "right to opt-out of ADMT" to delete "with respect to the consumer."	The Agency disagrees with this comment. The right to opt-out of ADMT is about opting out of the business's use of ADMT with respect to the consumer. The language is both necessary and clear regarding how the right to opt-out of ADMT works.
7001(bbb) [previously 7001(ccc)]	268, 368	Comment states that consumer privacy laws generally distinguish between users of a service who are over and under 13 years of age, rather than 16. Comment recommends adhering to that approach here. For minors over the age of 13, businesses should be able to design age-appropriate experiences tailored to their specific customer base.	The Agency disagrees with this comment. Including in the definition of sensitive personal information the personal information of consumers less than 16 years of age aligns the definition with California law, which gives additional protection to consumers 13 to 15 years of age. The comment provides no support for why defining sensitive personal information would hinder age-appropriate services for minors.
7001(bbb) [previously 7001(ccc])	416, 717	Comment states that § 7001(ccc) classifies personal information of minors under 16 as SPI. However, similar legislative attempts were vetoed by the Governor, so regulatory changes should not override legislative decisions.	The Agency disagrees with this comment. The CCPA clearly gives the Agency authority to add categories of sensitive personal information ("SPI"). (*See* Civ. Code § 1798.185(a)(1).) Adding minors' personal information to the definition of SPI aligns the definition with several other jurisdictions while also reflecting how California's law gives additional protections to consumers 13 to 15 years of age. The comment does not identify the

			specific bills to which it alludes or the accompanying veto messages to allow the Agency to respond to the specific bill.
7001(bbb) [previously 7001(ccc)]	578	Comment opposes categorizing all data concerning individuals under 16 as "sensitive personal information," arguing that this will force businesses to collect more data for age verification, contradicting privacy principles. Comment also contends that the Agency lacks statutory authority to redefine sensitive data this way.	The Agency disagrees with this comment. Adding minors' personal information to the definition sensitive personal information ("SPI") aligns the definition with several other jurisdictions while also reflecting how California's law gives additional protections to consumers 13 to 15 years of age. Also, the CCPA clearly gives the Agency authority to add categories of SPI. (*See* Civ. Code § 1798.185(a)(1).)
7001(bbb) [previously 7001(ccc)]	967	Comment suggests that the definition of SPI should explicitly include gender identity. Trans individuals face systemic discrimination in algorithmic decision-making systems, which must be acknowledged and addressed.	While not on the proposed action, the Agency notes comment's suggestion and looks forward to continuing to work with stakeholders on future policy development.
7001(bbb) [previously 7001(ccc)]	981	Comment indicates that the SPI definition should be revised to include neural data.	The Agency agrees with this comment and has added neural data in the definition of sensitive personal information.
7001(bbb) [previously 7001(ccc)]	1295	Comment advocates for explicitly classifying personal information of children under 16 as "sensitive" to ensure stronger privacy protections. Comment highlights the unique vulnerabilities of children and teens in digital spaces and argue that California's rules should align with other states.	The Agency agrees with this comment and notes comment's support.
7001(bbb) [previously 7001(ccc)]	1414	Commend recommends revising "sensitive personal information" definition to include the personal information of consumers that the business has actual knowledge are less than 13 years of age, instead of 16 years of age.	The Agency disagrees with this comment. Including in the definition of sensitive personal information the personal information of consumers less than 16 years of age aligns with the definition with California law, which gives additional protection to consumers 13 to 15 years of age.

7001(bbb) [previously 7001(ccc)]	1813	Comment suggests clarifying that messaging services outside of mail, email, and text messages, need to be included in the definition of sensitive personal information, as a proactive step to include communication formats that exist today and will be made available in the near future.	The Agency disagrees with this comment. The definition of "sensitive personal information" mirrors what is in the statute. It is reasonably clear with regard to the term "text messages," which is a generic term that would apply to all kinds of text messages, whether by SMS or messaging services. The Agency does not believe that further elaboration is necessary.
7001(bbb) [previously 7001(ccc)]	1824	Comment argues that legal counsel and/or professionals with a technical background will misunderstand § 7001(ccc) to only apply to individuals that have an established relation with the business.	The Agency disagrees with this comment. The definition of sensitive personal information mirrors what is in the statute. The use of the term "consumer" within the regulation is consistent with the language of the statute.
7001(eee)	579, 1415, 1712	Comment argues that the definition of "systematic observation" should be revised or deleted. Comment suggests narrowing the definition to exclude low-risk activities such as collecting data in public spaces where individuals are not specifically tracked, including geofencing and other passive data collection methods that do not involve profiling. Comment argues that the definition should exclude location tracking that consumers knowingly enable, such as through fitness apps or GPS-enabled services, as these are typically affirmatively chosen by users and already governed by device-level opt-in mechanisms. Comment warns that additional regulation could confuse users and duplicate existing safeguards. Comment recommends revising § 7001(eee) to state that "systematic observation" means methodical and regular or continuous observation a consumer has not chosen to enable, and to clarify that it does not include services that allow consumers to record their own movements. Comment proposes that the definition exclude location technologies that	The Agency disagrees with this comment. The definition of systematic observation is clear about what is in scope and addresses processing that presents significant risk to consumers' privacy based upon certain systematic observation. The regulations impose requirements upon businesses based upon their systematic observation of consumers. Comment's suggested revision is not more effective or appropriate than the Agency's regulation. Comment's recommendation would limit the definition to biological profiling and exclude many other processing activities that present significant risk to consumers' privacy.

		consumers enable on their mobile devices or in their cars. One comment recommends deleting the definition entirely.	
7001(eee)	1718	Comment suggests removing "or profiling" in the section.	The Agency disagrees with this comment because deleting "or profiling" would be less effective at protecting consumer privacy than the regulation by limiting the definition and excluding processing activities that present significant risk to consumers' privacy.
7001(fff)	227	Comment encourages the Agency to reconsider the regulations' requirements on training ADMT and AI and how such obligations will hamper companies' ability to thoroughly train their AI systems. If retained, § 7001's definition of training an ADMT or AI should be narrowed. At minimum, the regulations should only focus on narrow instances of training ADMT.	The Agency disagrees with this comment. However, the Agency revised the definition to align with revised risk-assessment requirements regarding training, and removed the definition's references to artificial intelligence as unnecessary.
7001(fff)	269	Comment suggests that fine-tuning should be excluded from § 7001(fff), as the regulations should regulate consumer-facing uses of ADMT, not companies' back-end internal operations.	The Agency disagrees with this comment. The Agency determined that adjusting parameters and improving algorithms are appropriately included in the definition of "train." In addition, the Agency has determined that a business processing personal information that the business intends to use to train ADMT for a significant decision, or to train certain technologies, presents significant risk to consumers' privacy. The regulations accordingly require a business to conduct a risk assessment for that processing. (*See* § 7150(b)(6).) However, the Agency revised the definition to align with revised risk-assessment requirements regarding training, and removed the definition's references to artificial intelligence as unnecessary.
7001(fff)	721	Comment argues that the problem with this provision is that the activities listed do not necessarily comport	The Agency disagrees with this comment. The definition is informed by approaches taken by other

		with what is generally understood to mean model training in the context of artificial intelligence. Although not subject to a single definition, the act of training a model is typically distinguished from operating the model. The former suggests that the model is learning or is modified in some way, while the latter need not result in a change to how the model will operate in subsequent uses.	agencies and regulators, such as the National Institutes of Standards and Technology and the Commission Nationale de L'informatique et des Libertés. However, the Agency revised the definition to align with revised risk-assessment requirements regarding training, and removed the definition's references to artificial intelligence as unnecessary.
7001(fff), 7200(a)	888	Comment suggests that the regulations should remove opt-out for uses of personal information to train ADMT or AI, because such training does not typically impact individuals directly. This opt-out could hinder AI development, introduce operational inefficiencies, and undermine AI's ability to provide unbiased and equitable outcomes. The CPPA should limit opt-out rights to cases where ADMT affects legally significant decisions.	The Agency disagrees with this comment. The regulations do not hinder development, introduce operational efficiencies, or undermine the ability of ADMT to provide unbiased and equitable decisions. However, the Agency has removed the opt-out requirement for training uses of ADMT to simplify implementation for businesses at this time.
Previous 7001(kkk)	966	Comment claims that the Agency's definition of "zero trust architecture" is misleading. The explanation should reflect the core principle that such systems do not store sensitive information, ensuring that user data cannot be leaked or mishandled.	The Agency disagrees with this comment. Nevertheless, the Agency deleted the term "zero trust architecture" to simplify implementation at this time.
Previous 7001(kkk)	1268	Comment supports the inclusion of Zero Trust Architecture (ZTA) in the proposed regulation, emphasizing its importance in minimizing implicit trust, reducing the risk of lateral movement, and preventing privilege escalation by threat actors. ZTA enhances security beyond traditional multifactor authentication (MFA) and baseline identity measures, making it a valuable addition to the regulation.	Agency agrees in part with this comment and notes comment's support. However, the Agency deleted the term "zero trust architecture" to simplify implementation at this time.
Previous 7001(kkk)	1417	Comment requests that the Agency delete "zero trust architecture" definition as unnecessary and that it is	The Agency disagrees with this comment. Nevertheless, the Agency deleted the term "zero trust

		inconsistent with other sections of cybersecurity audit. For example, the business must evaluate password authentication, but must also conduct an evaluation of zero trust architecture, which reflects a passwordless authentication protocol.	architecture" to simplify implementation at this time. In addition, the Agency deleted § 7123(b)(2)(C), which addressed zero-trust architecture, to simplify implementation at this time.

ARTICLE 1. GENERAL PROVISIONS – §§ 7002-7004

Section of Regulation	Comment Numbers	Summary of Comments 45-Day Comment Period	Agency Response
7002	313	Comment argues that the regulations should emphasize that businesses should only collect the minimum personal information necessary for specific purposes, explicitly linking data collection to its intended use.	The Agency disagrees with this comment. The CCPA and existing regulations set forth the standard of data minimization that businesses must comply with. (*See* Civ. Code § 1798.100(c), § 7002.) The Agency has determined that no further clarification is needed at this time.
7003	689	Comment argues that privacy disclosures should not be limited to manufacturers but must also be required of dealerships, insurance companies, and lenders. It suggests written, rather than oral, disclosures due to dealership personnel's lack of knowledge.	The Agency disagrees with this comment. Whether an entity must comply with the CCPA depends on whether it qualifies as a "business," "service provider," "contractor," or "third party" as those terms are defined by the statute. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. As to the method by which disclosures are made, the Agency applies a performative standard that gives businesses flexibility to craft a method that best fits their businesses' operations. The regulations are meant to be robust and applicable to many factual situations and across industries.
7003(c)	417, 722	Comment states that § 7003(c) changes "its homepage(s)" to "any internet webpage where personal information is collected," which introduces font and typeface requirements that are	The Agency disagrees with this comment. This is a non-substantive change because "homepage" has always been defined in the statute to include any internet webpage where personal information is collected. The

		unnecessary and burdensome. The previous language should be reinstated.	Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
7004	968	Comment supports the revisions to the regulations by the Agency.	The Agency agrees with this comment and notes comment's support.
7004(a)(2)(A)	369, 624, 685, 723	Comment suggests that the method for submitting CCPA requests and obtaining consent should be revised. The symmetry in choice requirement in § 7004(a)(2)(A) does not reflect the fact that there is an inherently different amount of work that is needed in order to opt-in (which can be done by clicking a single link) versus to opt someone out of sharing their information — for example, once they click the link, the business still needs to verify them. The regulations should revert to how they were previously drafted and require symmetry, but not limit opt outs to the "same or fewer" steps.	The Agency disagrees with this comment, which misstates the law. Opting-out of the sale/sharing of personal information is not a verifiable consumer request under the CCPA. The business should not be requiring verification for requests to opt-out of the sale/sharing of personal information. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
7004(a)(2), (3)	850	Comment appreciates simplification of the existing examples and the additional examples.	The Agency agrees with this comment and notes comment's support.
7004(a)(3)	818	Comment supports the subsection and advises a number of other things that comment believes constitute detrimental nudges, deceptive design, and dark patterns.	The Agency agrees with this comment to the extent that it supports the regulations and notes comment's support. Regarding the other items that the comment believes to be detrimental nudges, deceptive design, and dark patterns, the Agency does not believe that adding more examples is necessary at this time.
7004(a)(4)(C)	370, 625, 686, 724	Comment suggests that the method for submitting CCPA requests and obtaining consent should be revised. The prohibition in § 7004(a)(4)(C) on using general terms of acceptance conflicts with the CCPA which requires businesses to provide consumers with a notice at collection. This	The Agency disagrees with this comment, which appears to misunderstand the CCPA. The CCPA defines "consent" to mean "any freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer… signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose." (Civ. Code § 1798.140(h).) The definition goes on to say,

		prohibition does not relate to or address dark patterns and should be deleted.	"[a]cceptance of a general or broad terms of use, or similar document, that contains descriptions of personal information processing along with other, unrelated information, does not constitute consent." (Id.) The regulation is a restatement of the law in a way that makes it easier for businesses and consumers to understand. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
7004(a)(5)	626	The requirement mandating testing of these methods is duplicative and unnecessary as businesses already must comply with the requirements to offer functional and easy to use methods. The current statute and regulations provide the Agency and Attorney General's office the ability to investigate and penalize businesses for non-functional methods. Having a vague testing mandate only adds cost where businesses will test these methods as needed in order to provide functional methods for consumers to exercise their rights. We suggest utilizing a permissive structure instead of mandating testing.	The Agency disagrees with this comment. This modification clarifies requirements for businesses in designing and implementing methods for submitting CCPA requests. Testing a method to make sure that it functions is the most basic way to ensure that a method actually works. The regulation is not vague and should be understood by the plain language of the words. Moreover, the regulation provides examples that demonstrate how to comply with the requirement.
7004(a)(5)(C)	904	Comment suggests adding "unnecessarily" before the reference to multiple forms because there may be valid reasons for requiring consumers to fill out multiple forms. For example, allowing a customer to submit a request to both erase his personal data and have it updated in a single form submission would place a company in an unsensible position of needing to update the personal data immediately prior to erasing it. This would increase compliance costs on the industry with no benefit to data subjects.	The Agency disagrees with this comment. Adding "unnecessarily" is not necessary because the regulation already includes "unnecessarily" at the beginning of the sentence and "unnecessary" at the beginning of the subsection. Also, this is an example that illustrates what may be unnecessary burden or friction in the process. It is not meant to address every single factual scenario.

ARTICLE 2. REQUIRED DISCLOSURES TO CONSUMERS

Section of Regulation	Comment Numbers	Summary of Comments 45-Day Comment Period	Agency Response
7010, 7021, 7062, 7080	1523	§§ 7010, 7021, 7062, and 7080 impose burdensome requirements regarding pre-use notices, opt-outs, and access rights on test delivery systems that do not qualify as ADMT or involve personal data.	The Agency disagrees with this comment. The regulations cited by the comment explicitly reference ADMT, which is defined to include technologies that process personal information. To the extent that a business is using ADMT for a significant decision, it is subject to these requirements. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA.
7011(e)(1)	790	Comment asserts that requiring more information to provide a "meaningful understanding" of the parties to whom information is sold or shared could be akin to having to actually name the third party in privacy policies.	The Agency disagrees with this comment. The regulation is reasonably clear by the plain language of the words that a "category" is to be described, not an actual name of a third party. This phrase is used multiple times in preexisting subsections of the regulations and is not ambiguous.
7011(e)(1)	851	Comment indicates that §§ 7011(e)(1)(B) and (E) require that the categories of sources from which personal information is collected and the categories of personal information sold or shared to third parties "be described in a manner that provides consumers a meaningful understanding" of the sources and third parties. Because this standard is subjective, RMAI suggests that examples of descriptions that do and don't provide "meaningful understanding" would be helpful.	The Agency disagrees with this comment. The regulation is reasonably clear by the plain language of the words. This phrase is used multiple times in preexisting subsections of the regulations. The Agency does not think that adding examples is necessary at this time.
7012	312	Comment suggests that the regulations should offer flexible, practical guidance for providing Notice at Collection in various contexts. Businesses need clear guidelines for incorporating notices into a single	The Agency disagrees with this comment. § 7012 is reasonably clear and already provides flexible, practical guidance for how to provide Notice at Collection in various contexts. The Agency applies a performative

		step, such as within Terms of Service acceptance. Clarification is needed when third parties collect personal information on a business's platform.	standard to give businesses flexibility to craft methods that best fit their businesses' obligations.
7013(e)(3)	941	Comment asserts that the language used in 7013(e)(3)(C) is ambiguous and limits the flexibility businesses have in providing the notice most effectively. It would be more effective to not specify how the customers must encounter the notice.	The Agency disagrees with this comment. The purpose of the notice at collection is to provide consumers with timely notice, at or before the point of collection, so that consumers have a tool to exercise meaningful control over the business's use of their personal information. The examples provided are clear and necessary to provide businesses with clarity on how to provide such notices. They apply a performative standard that gives businesses flexibility to craft a method for providing notice as long as the consumer will encounter the notice before or at the time the device begins collecting the personal information. It is not more effective to not specify how customers must encounter the notice as the comment suggests.
7013, 7014	690	Comment recommends explicitly including "vehicles" in the list of examples where opt-out and limitation rights apply, ensuring that automotive businesses are explicitly covered under these provisions.	The Agency disagrees with this comment. The regulation is reasonably clear, and the Agency has determined that an additional example is not necessary at this time.
7013(e)(3), 7014(e)(3)	901	Comment argues that these prescriptive requirements do not provide enough flexibility for businesses to reach consumers with notices on different channels and through more accessible and consumer-friendly methods. They also do not consider changes in technology, which may not permit notices to be served through the medium that actually collects personal information to provide a service. Appropriate flexibility should be afforded to permit notices to be provided in ways that consumers will best receive and understand them. For example, smart speakers or other devices without screens may	The Agency disagrees in part with this comment, but has modified the regulation to clarify that the notice must be given before or at the time the personal information is collected, and in the augmented or virtual reality setting, before or at the time the consumer encounters the business collecting the personal information. The regulation applies a performative standard that gives businesses flexibility to craft a method for providing notice as long as the consumer will encounter the notice before or at the time the device begins collecting the personal information.

		be best suited to provide requisite notices through applications that accompany the device rather than through the speaker itself, as a written form of the notice may be easier for a consumer to review for pertinent information. Moreover, overly prescriptive requirements regarding methods of notice are likely to lead to increased administrative burdens, higher costs, and potential compliance issues, especially for small businesses. These costs will ultimately fall to consumers in terms of frustrated access to innovative offerings, new AR/VR tools, and new connected devices. Flexibility in the form of notice should be permitted to ensure that businesses can provide disclosures in ways that are helpful and logical for consumers.	
7013(e)(3), 7014(e)(3)	1863	Comment states that §§ 7013(e)(3)(D) and 7014(e)(3)(D) require privacy notices be provided before entering an immersive environment, which may be impractical. Comment also argues that the ISOR does not explain why a notice offered in an augmented or virtual reality environment is considered to be per se less effective than a notice conveyed outside an augmented or virtual reality environment. Comment recommends that the regulations should ensure flexibility in order to provide context-appropriate and timely notices, as regulations should focus on quality of notices, not necessarily the format in which notices are provided.	The Agency agrees in part with this comment. The Agency has modified the regulation to clarify that the notice must be given before or at the time the personal information is collected, and in the augmented or virtual reality setting, before or at the time the consumer encounters the business collecting the personal information. The regulation applies a performative standard that gives businesses flexibility to craft a method for providing notice as long as the consumer will encounter the notice before or at the time the device begins collecting the personal information.

ARTICLE 3. BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS

Section of Regulation	Comment Numbers	Summary of Comments 45-Day Comment Period	Agency Response
7020(e)	418	Comment argues that § 7020(e)'s requirements to allow consumers to request data beyond the statutory look-back period of January 1, 2022 conflicts with the statute. Businesses should not be required to provide information they no longer maintain due to standard data retention policies.	The Agency disagrees with this comment. The comment's interpretation of the regulation is inconsistent with the regulation's language. The regulation states that the obligation only applies if a business maintains personal information for longer than 12 months. Nevertheless, the Agency has modified the language to clarify that the use of the method is not required for personal information collected prior to January 1, 2022.
7020(e)	725	The regulation exceeds the scope of and contradicts the statute because the look back only applies to PI collected on or after January 1, 2022. The Agency can only require a date range for PI on or after January 1, 2022. Also, a business should be able to object to right to know on the basis that the information has already been purged or deleted in accordance with retention policies.	The Agency disagrees with this comment. Nevertheless, the Agency has modified the language to clarify that the use of the method is not required for personal information collected prior to January 1, 2022.
7020(e)	791	Comment requests that language be added to clarify that this only applies to PI collected on or after January 1, 2022.	The Agency agrees in part with this comment and has modified the language to clarify that the use of the method is not required for personal information collected prior to January 1, 2022.
7022	691	Comment proposes that data deletion requirements extend to vehicles, especially in cases like repossession or total loss claims. It recommends following the NIST 800-88 Rev. 1 guidelines for proper sanitization of data before vehicle resale.	The Agency disagrees in part with this comment. The current regulation applies a performative standard that gives businesses discretion in how to comply with the consumer's request in a manner that best fits their business operations. The Agency has determined that the regulation is reasonably clear and the Agency has not determined that the level of detail specific to this

			factual situation is not necessary at this time. The regulations are meant to be robust and applicable to many factual situations and across industries.
7022	958	Comment argues that the California legislature has explicitly considered and provided a mechanism for an analog of the "remains deleted" requirement through the Delete Act. The CCPA's drafters did not provide for a comparable mechanism that would allow businesses to ensure a consumer remains deleted without violating the requirement to fully comply with a deletion request.	The Agency disagrees in part with this comment. Nevertheless, the Agency has deleted this requirement to simplify implementation at this time.
7022(b)(1)	942	Comment indicates that the Agency should clarify that businesses are permitted to retain necessary records to ensure the effective execution of these measures. This clarification would help prevent unintended conflicts between the new requirements and existing processes for handling deletion requests. It would also align with the current exceptions to the deletion right.	The Agency disagrees with this comment. There is no need to provide this clarification because it already exists in § 7022(e), which states that a business, service provider, contractor, or third party may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from its records.
7022(b), (c)	956	Comment asserts that the practicalities of ensuring that a consumer's PI remains deleted in (b)(1) and (c)(1) are inconsistent with other clear requirements in the CCPA and the regulations. To ensure that a consumer's personal information "remain deleted" would appear to require that the business actually retain personal information about the consumer — i.e., for suppression purposes — instead of fully and completely deleting the consumer's personal information. However, the CCPA and its existing regulations require that a business respond to a verifiable consumer request to delete by permanently	The Agency disagrees with this comment. § 7022(e) already accounts for this issue by stating that a business, service provider, contractor, or third party may retain a record of the request for the purpose of ensuring that the consumer's personal information remains deleted from its records. Nevertheless, the Agency has deleted this language to simplify implementation at this time.

		and completely erasing the consumer's personal information from their systems.	
7022(b), (c), (f)	627	Requiring businesses, service providers, and contractors to take "measures" to ensure personal information "remains deleted" would impose an ambiguous and problematic standard. Businesses might be incentivized to retain more PI than they otherwise would. This could also cause businesses to interfere with or block a consumer who chooses to reengage with a business after requesting deletion. Statute requires deletion of personal information the business "has collected from the consumer," which applies only to data the business has already collected. The regulation can be read to transform this into a forward-looking requirement, prohibiting the business from collecting data going forward. The reg is problematic for service providers and contractors who are statutorily limited in their decision making vis-a-vis personal information. It exceeds the bounds of the service provider or contractor role to implement "measures" to prevent it from acting on the instruction of the business in such a situation, not to mention the confusion it would cause to many established business relationships and norms.	The Agency disagrees in part with this comment. Nevertheless, the Agency has deleted these provisions to simplify implementation at this time.
7022(b), (c), (f)	895	The Agency has not issued regulations that comply with its regulatory mandate and provided guidance regarding which signals that are available in the marketplace meet legally prescribed requirements. Thus, businesses would have to guess which signals are valid. The CPPA should ensure that any requirement to display the status of an opt-out preference signal is appropriately scoped through	The Agency disagrees with this comment. The Agency has issued regulations setting forth the requirements for an opt-out preference signal that must be honored by businesses. (*See* § 7025(b).) The Agency's previous rulemaking documents stated that the Global Privacy Control meets these requirements. Recognition of GPC as a valid OOPS has been reinforced by enforcement actions by both the Attorney General's office and the

		exceptions or limitations on enforcement to account for a lack of clarity regarding what constitutes a valid signal. The CPPA should also make clear that entities that offer OOPS must comply with the signals in the same way as other businesses. Implementing reasonable exceptions and clarifications to the requirement to display the status of an OOPS would help prevent unfair penalties. It would also help ensure businesses are not held accountable for signals that do not comply with law or circumstances that are beyond their control, thus balancing regulatory compliance with operational feasibility.	Agency. Colorado has also recognized GPC as a universal opt-out mechanism, which is Colorado's equivalent to CA's OOPS. Comment's continued arguments to the contrary lack merit. As to the requirement to display the status of the consumer's opt-out, it is necessary to avoid confusion for consumers on their opt-out state while using a business's website or online service.
7022(b), (c), (f)	896	Comment argues that this mandate should be clarified to apply to "previously collected personal information" rather than all personal information collected about a consumer on a going-forward basis to prevent the introduction of a new "do not collect" requirement and to ensure outdated information can be appropriately removed or filtered out of businesses' systems. Businesses may have legitimate reasons to do this. The current wording of the regulations could create unintended results, such as requiring businesses to keep outdated information in their systems despite learning new information to the contrary. Such a rigid requirement would cause significant consumer frustration when, for example, address changes and other new data elements are not able to be updated seamlessly in businesses' systems.	The Agency disagrees in part with this comment. Nevertheless, the Agency has deleted these requirements to simplify implementation at this time.
7022(b), (f)	905	Comment asserts that this language would significantly impede online commerce and prohibit the collection of personal information that is in line with both the expectation and intent of consumers. To	The Agency disagrees in part with this comment. Nevertheless, the Agency has deleted these requirements to simplify implementation at this time.

		comply with this requirement, a shipping company would need to scan every incoming shipment and turn away any order where the recipient had previously requested erasure of their personal information. Retailers would need to have relationships with multiple logistics providers and send the personal information to each company, one-by-one, until a logistics provider which has not yet received an erasure request from the recipient is found. This would increase costs on the retailer, the logistics company, and the consumer and introduce delays. At worst, the customer would be unable to receive their online purchases. Comment suggests a modification which would permit a business to accept personal information when the consumer interacts with the business subsequent to their deletion request.	
7022(f)	419, 726	Comment argues that § 7022(f)'s requirements exceed statutory authority, as the CCPA only grants the right to delete information collected directly from consumers.	The Agency disagrees in part with this comment. Nevertheless, the Agency has deleted this requirement to simplify implementation at this time.
7022(f)	792	Comment asserts that the language is overly burdensome because it imposes a responsibility that belongs to the SP or contractor on the business.	The Agency disagrees with this comment. Nevertheless, the Agency has deleted this requirement to simplify implementation at this time.
7022(f)	951, 957	Comment suggests that the Agency clarify that while a business may need to implement measures to prevent the recollection of data from third parties after a deletion request, this obligation does not extend to acts taken by consumers. Otherwise, it may go against the consumer's expectations. For example, if a consumer visits a website after making a deletion request, makes a purchase, or otherwise provides information or engages with a business in a manner	The Agency agrees in part with this comment. The Agency has deleted this requirement to simplify implementation at this time.

		that would result in the collection of personal information, that should not impact the determination that the business complied with the deletion request.	
7023(c)	852	Comment asserts that the CPPA should explain that the information provided by the consumer is not necessarily static and may itself warrant correction if it subsequently becomes inaccurate. Provides two examples.	The Agency disagrees in part with this comment. The Agency does not think that the comment's proposed language is necessary to clarify the regulation. The regulation is reasonably clear and the examples provided within the regulation already explain what is meant by the term "remains corrected."
7023(c)	906	Comment indicates that the suggested language would significantly slow online commerce and impede consumers in sending their parcels to different addresses. Consumers know logistics providers will ship an online purchase to the address the individual provides at checkout. They would expect to receive the parcel at the provided address, regardless of whether they are permanently associated with the destination address. This language would require a logistics provider to scan every incoming shipment, cross reference it against a list of consumers who have submitted a consumer request to correct their personal information, and proactively reach out to the consumer when the destination address does not match information they submitted in their correction request. Otherwise, the business may be deemed to have not implemented "measures to ensure that the information remains corrected." At a minimum, this would increase costs. At worst, consumers may not receive urgent parcels when needed, even if an expedited shipping level is selected. Suggest modifying text to permit a business to accept personal information as being accurate when the consumer provides such personal	The Agency disagrees in part with this comment. Nevertheless, the Agency has deleted this requirement to simplify implementation at this time.

		information to the business subsequent to his or her correction request.	
7023(c), 7023(k)	897	Comment asserts that this mandate should be clarified to apply to "previously collected personal information" rather than all personal information collected about a consumer on a going-forward basis to prevent the introduction of a new "do not collect" requirement and to ensure outdated information can be appropriately removed or filtered out of businesses' systems. Businesses may have legitimate reasons to do this. The wording of the regulations could create unintended results, such as requiring businesses to keep outdated information in their systems despite learning new information to the contrary. Such a rigid requirement would cause significant consumer frustration when, for example, address changes and other new data elements are not able to be updated seamlessly in businesses' systems.	The Agency disagrees with this comment. The Agency does not think that the comment's proposed clarification is necessary. The regulation is reasonably clear and the examples provided within the regulation already explain what is meant by the term "remains corrected."
7023(c), 7023(f)(3), 7023(i), 7023(j)	414, 715, 728, 729	Comment argues that several amendments impose significant compliance costs but do not meaningfully enhance consumer protections. Specifically, §§ 7023(c), 7023(f)(3), 7023(i), and 7023(j) require businesses to tag metadata at the individual data element level. This approach is costly, operationally burdensome, and redundant given existing data processing regulations.	The Agency disagrees with this comment. The modifications and examples provided benefit both consumers and businesses in ensuring that personal information maintained by the business is accurate and not overwritten by incorrect information, which would render the request obsolete. Businesses also benefit by having accurate information. Nevertheless, the Agency has deleted the requirements in § 7023(f)(3) to simplify implementation at this time.
7023(c), 7023(f)(3), 7023(i), 7023(j)	420	Comment asserts that §§ 7023(c), 7023(f)(3), 7023(i), and 7023(j) impose excessive data tracking requirements, including: ensuring corrected data remains accurate indefinitely, and tracking the status and source of individual data elements. These	The Agency disagrees with this comment. The Agency has explicit authority to adopt regulations regarding how a business responds to a request to correct. (*See* Civ. Code § 1798.185(a)(6), (7).) The regulations and examples provided benefit both consumers and

		requirements are costly, offer minimal consumer benefit, and exceed statutory intent.	businesses in ensuring that personal information maintained by the business is accurate and not overwritten by incorrect information, which would render the request obsolete. Businesses also benefit by having accurate information. Nevertheless, the Agency has deleted the requirements in § 7023(f)(3) to simplify implementation at this time.
7023(f)(3)	372, 629, 687	Comment suggests that requests to correct should be revised. The draft regulations require that, if a business denies a right to correct, it must then inform the consumer that it will note both internally and to third parties to whom it disclosed the personal information that the accuracy of the PI is contested. This provision goes beyond the scope of the law and should be deleted. The CCPA provides for an obligation to correct and exception to that obligation. The CPPA should not place additional and burdensome requirements on businesses that will not be practical to operationalize.	The Agency disagrees with this comment. The Agency has explicit authority to adopt regulations regarding the consumer's right to correct. (*See* Civ. Code § 1798.185(a)(6), (7).) Nevertheless, the Agency has deleted these requirements to simplify implementation at this time.
7023(f)(3)	730	Comment believes this provision goes beyond the scope of the law and should be removed from the final rules.	The Agency disagrees with this comment. However, the Agency has deleted this provision to simplify implementation at this time.
7023(f)(3)	907	Comment asks that the Agency amend the language to include that a business does not need to respond to abusive or non-verifiable requests.	The Agency disagrees with this comment. § 7027(m)(2)(B) is an example of a type of use of sensitive personal information that would fall within the listed exception to the right to limit. The Agency has determined that no further clarification is needed at this time. Examples do not need to reflect all instances in which a business may fall within this exception.
7023(i)	731	Requiring businesses to track, at the specific, individual data element-level, the source of the individual data element and, upon receipt of a	The Agency disagrees with this comment. This regulation is necessary to prevent the further proliferation of inaccurate information about the

		request to correct, either provide the name of the source of the data element to the requesting consumer or else inform the source of the data element imposes too great a burden on business. The cost to implement such specific, individual data element-level controls far outweighs the marginal consumer benefit that the CPPA seeks in proposing this change.	consumer and to give the consumer the ability to remedy the incorrect information at its source. The benefits outweigh the costs of this change.
7023(i)	898	Comment suggests that businesses should not be required to disclose the names of their partners and customers. Maintaining the optional nature of the present rule would help avoid anti-competitive effects, ensure businesses can continue to meet confidentiality requirements they may be subject to through contracts with their data sources, and protect trade secrets.	The Agency disagrees with this comment. This regulation is necessary to prevent the further proliferation of inaccurate information about the consumer and to give the consumer the ability to remedy the incorrect information at its source. Businesses have the option of informing their sources directly instead of disclosing this information to consumers, thus addressing the comment's concerns about trade secrets and anti-competitive effects.
7023(k)	421, 733	Comment states that § 7023(k)'s requirement goes beyond statutory intent, which only requires "commercially reasonable efforts." Consumers already have mechanisms to verify and correct their data, such as requests to know and privacy policy disclosures.	The Agency disagrees with this comment. The Agency has explicit authority to adopt regulations regarding how a business responds to a request for correct. (*See* Civ. Code § 1798.185(a)(6), (7).) The regulations and examples provided benefit both consumers and businesses in ensuring that personal information maintained by the business is accurate and not overwritten by incorrect information, which would render the request obsolete. Businesses also benefit by having accurate information.
7023(j)	732	Requiring businesses to provide a means by which a consumer might confirm that the personal information the business maintains is the same as what the consumer provided imposes too great a burden on businesses. Through the consumer right to know, the statute already provides consumers with	The Agency disagrees with this comment. This regulation is not redundant. It is necessary to harmonize the regulation with the business's processes for responding to requests to correct. If the business is required to provide a way to confirm that sensitive personal information maintained about the consumer is

		such a method to confirm the accuracy of the information that the business maintains. Building in redundant requirements merely serves to increase the compliance burden (and expense) on businesses without any meaningful additional benefit to consumers.	correct, it should provide consumers a way to do so in response to request to know.
7023(j), 7024(d)	899	Comment requests that the Agency clarify acceptable "ways" businesses can meet this new requirement while minimizing the possibility of exposing sensitive data elements to fraudsters or others who are not the consumer to which the personal information pertains. To protect sensitive personal information from unnecessary exposure and to provide meaningful clarity, the CPPA should state that businesses may satisfy this requirement by confirming the type of data elements they maintain or by confirming redacted or truncated portions of the information to reduce the potential for unnecessary data leakage.	The Agency agrees in part with this comment and has provided an example of how a business can confirm that the sensitive personal information it maintains is the same as what the verified consumer has provided.
7024(d)(2)	373, 630, 688	Comment suggests that requests to know should be revised. The draft regulations require businesses to provide consumers with a way for consumers to confirm that SPI information is the same as what the consumer expects it to be, while also prohibiting businesses from disclosing such SPI. It is unclear to comply with this requirement without disclosing such information.	The Agency disagrees with this comment. The regulation is reasonably clear and applies a performative standard that gives businesses flexibility to craft a method that best fits their business operations. Nevertheless, the Agency has added an example of a way in which a business may comply with this regulation.
7024(d)(2)	422, 734	Comment states that § 7024(d)(2) introduces redundant obligations by requiring businesses to provide a way for consumers to confirm their stored data matches their records duplicates existing right to know and right to correct provisions. The existing	The Agency disagrees with this comment. This regulation is not redundant. It is necessary to harmonize the regulation with the business's processes for responding to requests to correct. If the business is required to provide a way to confirm that sensitive personal information maintained about the consumer is

		right to know and right to correct already address this need.	correct, it should provide consumers a way to do so in response to request to know.
7024(d)(2)	943	Comment asserts that this requirement is at odds with the prohibition in § 7024(d) that prevents businesses from providing certain sensitive information to consumers, which is designed to protect against fraud. The CPPA should resolve this tension by removing § 7024(d)(2) to avoid undermining important consumer fraud protections.	The Agency disagrees with this comment. Businesses can comply with this regulation without undermining fraud protections. The Agency has provided an example of how this can be done.
7024(e)	75, 76	Comment seeks clarification on whether businesses must provide a detailed legal citation when denying a request due to a legal conflict in § 7024(e). They ask whether businesses should reference specific laws and regulations to ensure transparency and consistency. Asks if a general statement about a legal conflict would suffice. Clear guidance will improve transparency for consumers and help businesses comply with the new requirements.	The Agency disagrees with this comment. The Agency has adopted a performance standard to allow businesses with flexibility to determine how to meet the requirement that best fits their business operations. The Agency has determined that it is not necessary to require a prescriptive standard to effectuate the purpose and intent of the CCPA.
7024(k)(6), 7024(*l*)	631	There is little consumer benefit from requiring a business to disclose the categories of service providers or contractors to which it discloses personal information. By definition, these entities step into the shoes of a business and perform services on such businesses' behalf, with no autonomy as to the purposes or means of processing consumers' personal information. Businesses must already account for all their processing activities in their privacy policy, notice at collection, and in response to a consumer's request to know by explaining the "purpose for which it collected" personal information. Furthermore, when engaging a service provider or contractor, a business must adopt many protections, such as stringent contractual	The Agency disagrees in part with this comment. The CCPA requires businesses to provide the categories of service providers or contractors to which it discloses personal information. (*See* Civ. Code § 1798.130(a)(4)(C).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.

		requirements to ensure such vendor operates at the business's instruction and consistent with the business's obligations under the CCPA. Thus, it is immaterial to a consumer whether a processing activity is carried out by the business directly or by its designated service provider or contractor, since the business bears ultimate responsibility for the activity in either instance.	
7025	310	Comment suggests that the provisions for "Do Not Sell or Share My Personal Information" links and opt-out mechanisms should account for the feasibility for small-to-medium businesses. Comment requests clarification on how to handle situations where third-party platforms update their practices and how that affects a business's compliance requirements. It requests clearer instructions and guidance on what qualifies as an OOPS and how to implement OOPS.	The Agency disagrees with this comment. The regulations are reasonably clear regarding how to implement opt-out mechanisms, including with regard to businesses' obligations regarding third parties. They set forth the requirements for signals that should be recognized and how the business is to respond to said signals. They also provide several examples. To the extent that the comment seeks exceptions for small-to-medium size businesses, this is inconsistent with the CCPA, which requires all entities that qualify as a "business" to provide opt-out links and comply with opt-out requests. (*See* Civ. Code § 1798.135.) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
7025	316	Comment requests clear examples and thresholds to define "disproportionate effort" when responding to consumer requests. It should be made clear if the cost to the business or other measures of resources required to comply with the regulations can be considered in determination of "disproportionate effort."	The Agency disagrees with this comment. "Disproportionate effort" is defined by § 7001(m) and is reasonably clear. The Agency does not believe it will add clarity to provide examples and it may be too limiting.
7025	692	Comment proposes expanding opt-out mechanisms beyond the GPC to include other consumer-friendly	The Agency agrees in part with this comment. However, the Agency has determined that adding specifications for additional opt-out mechanisms is not necessary at

		signals like OptOutCode, which allows consumers to mark devices as opted out via renaming functions	this time. It is continually watching the development of these types of tools.
7025	1797	Comment argues that Global Privacy Control (GPC) signals are unclear about what consumers are opting out of, who I am opting out from, and how consumers can be adversely impacted by opting out. When using a GPC signal, I need to know if I am opting out of sale, ADMT, training of ADMT, re-publishing of PI, or targeted advertising. Comment also suggests that businesses may claim to comply with the CCPA by putting the DO NOT SELL MY PERSONAL INFORMATION link on their website and state that they don't sell or share personal information. However, both statements could be false.	The Agency disagrees in part with this comment. The regulations are reasonably clear about disclosures and requirements relating to opt-out preference signals (OOPS), like the GPC. OOPS apply to the sale and sharing of personal information, not ADMT or the training of ADMT. The methods for opting out of ADMT are the subject of this rulemaking package and have not yet been operationalized. The regulations also set forth the requirements of what disclosures about the sale/sharing of personal information must include. For example, the CCPA requires businesses to identify by category (not by name) the third parties to whom they sell or share personal information. Regarding businesses placing a DNSS link while also stating that they do not sell or share personal information, this is not a topic of this rulemaking. Whether such statements are true or false is a fact-specific inquiry and related to enforcement, not any of the regulations.
7025(c)(6)	684	Comment opposes requiring business to display whether it has processed an OOPS. It would reverse the purpose of streamlining the user experience and will create a new screen for the consumer to click through, undoing the frictionless use case.	The Agency disagrees with this comment. This regulation is necessary to avoid confusion for consumers on their opt-out state while using a business's website or online services. It gives consumers the ability to know that the signal is being consistently applied across the different websites they visit and engenders confidence in the opt-out preference signal preventing the sale or sharing of their personal information. There is nothing in the regulation that requires a new screen or pop-up that would undo the frictionless use case.
7025(c)(6)	878	Comment argues that the requirement to display status of opt-out is inflexible. It should be modified to	The Agency disagrees in part with this comment. This subsection is an example and does not reflect all factual

		recognize that two interfaces for displaying opt-out status may not always be logical or feasible depending on the service in question.	scenarios that would be in compliance with this requirement.
7026	693	Comment proposes adding an illustrative example clarifying that even anonymized geolocation data from vehicles, when shared with third parties, constitutes a "sale" under CCPA if re-identifiable.	The Agency disagrees in part with this comment. The regulation is reasonably clear and adding another example is not necessary at this time. Whether something is a sale is a very fact-specific analysis.
7026	309	Comment argues that the definition of "sharing" under the CCPA is ambiguous, particularly regarding third-party analytics platforms like Google Analytics. The regulations should clearly distinguish between internal analytics and "cross-context behavioral advertising" and specify whether de-identified or aggregated data falls under the scope of "sharing." Additionally, a carve-out for sharing personal information within the context of user interaction in social networks is necessary for functionality.	The Agency disagrees with this comment. The definition of "sharing" is set forth in the CCPA and is reasonably clear when read together with other definitions, such as "personal information" and "cross-context behavioral advertising." The definition of "personal information" specifically addresses whether de-identified or aggregate data is within the scope of "sharing." The Agency cannot amend definitions in the CCPA or adopt regulations inconsistent with the CCPA. The Agency has determined that no further clarification, including regarding a safe harbor, is needed at this time.
7026(f)(3)(A)	893, 944, 952	Comment indicates that complying with consumer requests to opt out of sale and sharing "immediately" in a programmatic advertising setting is too rigid to account for internal operations and common realities associated with coordinating opt outs with other businesses. It ignores batched suppression list update processes that many programmatic advertising vendors regularly employ. Processes for data flows between providers, such as how often businesses send data to other entities or to end platforms for sales or sharing, vary significantly. Many vendors in the real-time-bidding space may update their suppression lists to account for opted-out users on a weekly basis. The current regulatory scheme already requires businesses to "notify" all	The Agency disagrees in part with this comment. This subsection is an example and does not reflect all factual scenarios that would be in compliance with this requirement. Nevertheless, the Agency has revised the example to make clear that the business in this example is capable of restricting the transfer of personal information instantaneously.

		third parties who may have received personal information after the business received an opt-out request that a consumer had made an opt-out request. This requirement to notify any third parties who received personal information after a consumer's optout request effectively ensures no personal information will be subject to further sales and sharing after a business receives a consumer's opt-out selection. The "immediate" timing unreasonably singles out one type of entity in the marketplace to be subject to more aggressive compliance requirements.	
7026(g)	945	Comment asserts that requiring businesses to provide consumers with a means to confirm that their opt-out request has been processed goes beyond the statute. It would be more appropriate to retain the optional nature of this action.	The Agency disagrees with this comment. The Agency has explicit authority to adopt regulations to establish rules and procedures to facilitate and govern business compliance with a consumer's opt-out request, as well as with regard to an opt-out preference signal, among other things. (*See* Civ. Code § 1798.185(a)(4), (18), (19).) This requirement is necessary to avoid confusion for consumers on their opt-out state while using a business's website or online service.
7027(m)	795	Comment expresses concern that the second sentence of 7027(m)(2)(B) implies that a business must do more than provide a notice to employees that their systems and technologies are monitored for information security purposes in order to satisfy this requirement.	The Agency disagrees with this comment. § 7027(m)(2)(B) is an example of a type of use of sensitive personal information that would fall within the listed exception to the right to limit. It makes no mention of notice to employees. The comment misinterprets the plain language of the regulation.
7027(m)	910	Comment suggests modifications to 7027(m)(2)(B) because a business may need to scan employees' outgoing emails for other purposes, such as preventing employees from leaking security credentials.	The Agency disagrees with this comment. § 7027(m)(2)(B) is an example of a type of use of sensitive personal information that would fall within the listed exception to the right to limit. The Agency has determined that no further clarification is needed at this

			time. Examples do not need to reflect all instances in which a business may fall within this exception.
7027(m)	969	Comment recommends including the word "sole" before "purpose" in the example in 7027(m)(2)(B) because it's unclear whether ancillary uses/information uncovered in the scanning for the allowed purpose are prohibited or not.	The Agency disagrees with this comment. § 7027(m)(2)(B) is an example of a type of use of sensitive personal information that would fall within the listed exception to the right to limit. The Agency has determined that no further clarification is needed at this time.
7027(m)	784	Comment indicates that § 7027(m)(3)(B) states that businesses may collect and use employees' biometric information to authenticate access for authorized people to secure areas of the workplace, but may not retain this information indefinitely or use it for unrelated purposes. Only the latter example, § 7027(m)(3)(B), specifies that the collected information cannot be reused for other purposes. To make sure that businesses understand the limits of § 7027(m)(2)(B), the final regulations should clarify that in both examples, collected information cannot be reused for other purposes.	The Agency disagrees in part with this comment. The suggested clarification is unnecessary as § 7027(m) already states that for all the exceptions, the business must only use and disclose the sensitive personal information for those purposes, and that the use and disclosure must be reasonably necessary and proportionate for those purposes.
7004, 7025, 7026, 7027, 7028	376, 377, 378, 379, 380, 381, 382, 383	Comment highlights its experience in automatic opt-out signals and proposes using its "Personal Data Choice Management Platforms" (PDCMPs) as an alternative to traditional consent management platforms. Comment argues that PDCMPs allow users to share their privacy preferences in advance and streamline consent requests. Comment claims that current 7004 requirements contributed to "consent fatigue" and that PDCMPs are a better method. Comment details why PDCMPs comply with the regulations and advocates for explicit recognition of	The Agency disagrees with the intent of this comment. This comment appears to seek the Agency's approval of its consent management platform as a method for submitting CCPA requests and obtaining consent. The Agency has adopted a performance standard to allow businesses with flexibility to determine how to meet the requirement that best fits their business operations. The Agency has determined that it is not necessary to provide an example of a compliant consent management platform. Moreover, whether the comment's consent management platform is compliant with the regulations is a fact-specific analysis.

		PDCMPs in the regulatory text as an example of an acceptable method for submitting opt-out requests.	
7022(g)(5), 7024(e)(3), 7026(e)	371, 374, 628, 727, 735	Requiring businesses to provide consumers a disclosure that they can file a complaint with the CPPA even if there are valid reasons for denial is counterintuitive and will result in unfounded complaints from consumers who interpret the complaint disclosure as a required next step. Therefore, this provision should be removed.	The Agency disagrees with this comment. Nevertheless, the Agency has deleted these requirements to simplify implementation at this time.
7022(g)(5), 7023(f)(6), 7024(e)(3), 7026(e), 7027(f)	793	The notice language should be modified so as not to presume that there has been a violation nor make legal conclusions. Should be modified to say, "If you believe your request has been denied without a valid reason…"	The Agency disagrees with this comment. Nevertheless, the Agency has deleted these requirements to simplify implementation at this time.
7025(c)(6), 7026(g), 7027(h)	894	The opt-out preference signal contravenes clear legislative text that makes honoring such signals optional. The CCPA itself therefore gives businesses the choice to either allow consumers to opt out through a do-not-sell link on their homepage(s) or through user-enabled global privacy controls. The Agency unilaterally read this option out of the law by requiring all businesses to adhere to optout preference signals. This regulation seeks to further entrench this interpretation, and thus, is contrary to the text of CA law.	The Agency disagrees with this comment. The comment proposes an interpretation of the CCPA that is inconsistent with the language, structure, and intent of the CCPA. The CCPA does not provide businesses with a choice between either posting opt-out links under Civil Code § 1798.135(a) or recognizing opt-out preference signals under § 1798.135(b). Rather, the choice is between posting opt-out links and frictionless processing of opt-out signals — that is, businesses cannot respond to the signal with a less functional website or product and cannot inundate the consumer with pop-up notifications. (*See* Civ. Code § 1798.135(b)(1) (citing Civ. Code § 1798.185(a)(19) as opposed to (a)(18).) A business may either (1) post opt-out links and for example, respond to an opt-out preference signal with a popup (subject to other limitations, such as the prohibition on using dark patterns to obtain consent, *see* § 7004(b)); or (2) the business can choose to not post opt-out links, but it then must process opt-out

			preference signals in a frictionless manner as set forth in § 7025(e) and (f).
7025(c)(6), 7026(g), 7027(h)	895	The Agency has not issued regulations that comply with its regulatory mandate and provided guidance regarding which signals that are available in the marketplace meet legally prescribed requirements. Thus, businesses would have to guess which signals are valid. The CPPA should ensure that any requirement to display the status of an opt-out preference signal is appropriately scoped through exceptions or limitations on enforcement to account for a lack of clarity regarding what constitutes a valid signal. The CPPA should also make clear that entities that offer OOPS must comply with the signals in the same way as other businesses. Implementing reasonable exceptions and clarifications to the requirement to display the status of an OOPS would help prevent unfair penalties. It would also help ensure businesses are not held accountable for signals that do not comply with law or circumstances that are beyond their control, thus balancing regulatory compliance with operational feasibility.	The Agency disagrees with this comment. The Agency has issued regulations setting forth the requirements for an opt-out preference signal that must be honored by businesses. (*See* § 7025(b).) The Agency's previous rulemaking documents stated that the Global Privacy Control meets these requirements. Recognition of GPC as a valid OOPS has been reinforced by enforcement actions by both the Attorney General's office and the Agency. Colorado has also recognized GPC as a universal opt-out mechanism, which is Colorado's equivalent to CA's OOPS. Comment's continued arguments to the contrary lack merit. As to the requirement to display the status of the consumer's opt-out, it is necessary to avoid confusion for consumers on their opt-out state while using a business's website or online service.

ARTICLE 4. SERVICE PROVIDERS, CONTRACTORS, AND THIRD PARTIES

Section of Regulation	Comment Numbers	Summary of Comments 45-Day Comment Period	Agency Response
7050(a)(3)(B)	903	Classifying a transportation/logistics company as a "service provider" for data privacy purposes imposes outsized burdens on our industry in light of the unique regulatory and legal environment in which we operate. This classification improperly	The Agency disagrees with this comment. This subsection is an example and does not reflect all factual scenarios, nor does it imply that a transportation/logistics company must be a service provider in all circumstances. Whether an entity is a "service provider" and/or a "business" requires a fact-specific analysis.

		discounts the fact that our member companies are public facing "businesses" with direct consumer relationships in their own right.	
7050, 7051	1802	Comment states that one of the regulations currently in effect requires every business covered by the CCPA to have written contracts with service providers, contractors, and third parties that process consumers' personal information. However, consumers are not provided access to even minimal information like the date of the agreement.	While not on the proposed action, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
7051	311	Comment argues that the Agency should address the limitations of enforcing compliance through contracts with third parties. Businesses have limited control over how third parties behave despite contractual obligations. The regulations should clarify how a business should proceed if a service provider violates CCPA terms and should provide standardized contract language. Additionally, service providers should notify businesses when they can no longer meet CCPA obligations. Guidance is needed on what constitutes "reasonable and appropriate steps" for ensuring compliance by service providers.	The Agency disagrees with this comment. The CCPA and its implementing regulations are reasonably clear regarding businesses' obligations regarding its relationship with third parties and service providers. Civil Code §§ 1798.100 and 7050-7053 of the regulations explicitly set forth the requirements for contractual language. The Agency applies a performative standard for contractual provisions to give businesses flexibility to craft language that best fits their business obligations. The Agency also provides examples of how a business can conduct due diligence over service providers and third parties. § 7051(a)(7) already addresses the service provider's requirement to notify the business if it can no longer meet its obligations under the CCPA and its regulations.
7051	736	The continued "tinkering" with the content requirements for the Service Provider/Contractor Addendum template creates substantial and unnecessary operational effort without any meaningful	The Agency disagrees with this comment. The regulations add examples of requirements that a business may include in its contracts with service providers or contractors relating to the business's cybersecurity audit, risk assessment, or complying with the business's ADMT requirements. (*See* § 7051(a).)

		increase to consumer privacy protection. Every time a change is made to the content requirements, a business seeking to comply must not only revisit their addendum template to ensure compliance for future engagements, but it must also revisit existing service provider/contractor relationships to determine which existing contract frameworks must be updated. This process of updating requires substantial time and effort, including efforts not only to coordinate execution, but to educate service providers/contractors about the need for such new language. As a result, for those businesses of a meaningful size that have dozens if not hundreds (or thousands) of service provider/contractor relationships, such an exercise can take months, if not longer, all with little marginal improvement and impact on consumer protection.	Adding these examples is consistent with the CCPA's direction to provide guidance to businesses regarding their duties and responsibilities. (*See* Civ. Code 1798.199.40(f).) It is also consistent with the CCPA's direction to the Agency with respect to the cybersecurity audit, risk assessment, and ADMT regulations. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security to perform a thorough and independent annual cybersecurity audit. The CCPA also directs the Agency to require businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment and submit it to the Agency on a regular basis. (Civ. Code § 1798.185(a)(14).) The CCPA further directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, it is required to issue regulations and impose certain requirements on this topic. Also, the Agency has appropriately considered the impact on businesses and innovation and has made efforts to limit the burden of the regulations while implementing the CCPA. The Agency engaged in robust preliminary and formal rulemaking activities with a wide variety of stakeholders and has collaborated with lawmakers and will continue to do so, consistent with the CCPA's direction to the Agency. (*See* Civ. Code § 1798.199.40(g).) Other changes to § 7051 — deleting subsection (a)(4) as duplicative, and deleting the clause "depending upon the circumstances" as unnecessary from subsection (c) — are not substantive or would not require revisiting an addendum.

DRAFT

ARTICLE 5. VERIFICATION OF REQUESTS

Section of Regulation	Comment Numbers	Summary of Comments 45-Day Comment Period	Agency Response
7060	315	Comment suggests that the regulations should clarify reasonable steps for verifying consumer requests and provide detailed guidance on thresholds for "reasonably high certainty." Businesses need direction on handling unverified requests and appropriate time frames for implementing verification measures.	The Agency disagrees with this comment. §§ 7060-7061 are reasonably clear and provide businesses the necessary guidance for how to handle the verification of consumer requests, including what is meant by "reasonable" and "reasonably high" degrees of certainty. The Agency has adopted a performance standard to allow businesses flexibility to determine how to meet the verification requirements in a way that best fits their business operations. Also, § 7021 clearly sets forth the timing requirements. The Agency has determined that no further clarification is needed at this time.
7060	694	Comment argues that businesses requiring notarized verification of privacy requests should compensate consumers for both the notary fees and their time.	The Agency disagrees with this comment. The Agency has determined that additional restrictions are not necessary at this time. The Agency applies a performative standard that gives businesses flexibility to craft their verification methods in a manner that best fit the nature of the personal information at issue.
7060	1779	Comment suggests that businesses should be encouraged to adopt cryptographic verification methods, multi-factor authentication (MFA), and risk-based authentication as alternatives to requesting additional consumer data. The Agency should explicitly recognize that automated verification tools, including identity validation APIs, public-private key authentication, and zero-knowledge proofs, can meet compliance requirements while reducing consumer data exposure. Comment seeks clarity on ADMT-driven verification and additional safeguards to prevent businesses	The Agency disagrees in part with this comment. The verification regulations set forth a performative standard that gives businesses flexibility to craft verification methods that best fit their business operations while considering factors like the type, sensitivity, and value of the personal information it collects and maintains, the risk of harm posed by unauthorized deletion, correction, or access to the information, among other things. The Agency does not think it is necessary to explicitly recognize specific verification tools at this time.

		from repurposing verification data for secondary uses, such as marketing, profiling, or behavioral tracking.	
7060	1780	Comment argues that the requirement for businesses to reimburse consumers for notarization costs is an unnecessary administrative burden that overlooks the need for digital identity verification alternatives. Instead, businesses should be encouraged to use secure digital methods like e-signatures, identity wallets, and decentralized solutions. The Agency should clarify that notarization can only be required if no reasonable alternative verification method is available.	The Agency disagrees in part with this comment. The verification regulations set forth a performative standard that gives businesses flexibility to craft verification methods that best fit their business operations while considering factors like the type, sensitivity, and value of the personal information it collects and maintains, the risk of harm posed by unauthorized deletion, correction, or access to the information, among other things. The Agency does not think it is necessary to adopt specific rules around notarization at this time.
7060	1781	Comment suggests that businesses should be permitted to implement enterprise-wide verification frameworks to ensure consistency across different business units and minimize redundant verification requests.	The Agency disagrees in part with this comment. The comment misinterprets the regulation. The verification regulations set forth a performative standard that gives businesses flexibility to craft verification methods that best fit their business operations. There's nothing in the regulations that prohibits a business from implementing enterprise-wide verification frameworks.
7060(b)	270	Comment suggests that this section should clarify that businesses must honor verifiable requests. Doing so would make this section consistent with language in the statute to facilitate verification tools that ensure users' actual preferences are applied.	The Agency disagrees with this comment. The comment is not about the substance of this regulation, which explains that businesses shall not require a consumer to verify their identity for certain requests to opt-out or limit. Making the requested change in this context would be confusing and unnecessary because requests to opt-out and limit are not verifiable requests according to the statute.

ARTICLE 8. TRAINING AND RECORD-KEEPING

Section of Regulation	Comment Numbers	Summary of Comments 45-Day Comment Period	Agency Response
7102(a)(1)(D), (G)	1418	Comment asserts that the Agency should delete the number of requests to access ADMT and requests to opt-out of ADMT.	The Agency disagrees with this comment. The regulation is necessary to inform the Agency, the Attorney General, and members of the public about businesses' compliance with the CCPA.

ARTICLE 9. CYBERSECURITY AUDITS

Section of Regulation	Comment Numbers	Summary of Comments 45-Day Comment Period	Agency Response
7120	192, 350, 638, 708, 1098	Comment argues that the applicability threshold is too low, both in terms of the breadth of businesses as well as the type of activities deemed a significant risk. Comment suggests that the Agency instead focus its audit requirements on activities that pose significant risk to the most sensitive data. Comment further argues that the cybersecurity audit threshold should be linked to data that presents an actual risk if compromised, rather than a broad numerical threshold. Comment proposes using the definition of personal information in California's data breach notification law (Civ. Code § 1798.82(h)) for consistency. Comment requests that § 7120(b) be revised to apply to businesses that process the personal information, as defined in California Civil Code §1798.82(h), of 250,000 or more consumers or households in the preceding calendar year. On the other	The Agency disagrees with this comment. The CCPA requires the Agency to consider the size and complexity of the business, and the nature and scope of its processing activities, in determining whether a business's processing of consumers' personal information presents significant risk to consumers' security. § 7120(b)(1)—deriving 50 percent or more of annual revenues from selling or sharing consumers' personal information—reflects the nature and scope of a business's processing activities, and can be a proxy for the business's complexity. § 7120(b)(2)(a) and (b)—the revenue and personal-information processing thresholds—reflect the business's size and complexity and the nature and scope of its processing activities. The Agency has determined that processing the personal information of 250,000 or more consumers, or the sensitive personal information of 50,000 or more consumers, presents significant risk to consumers' security. The criteria in § 7120(b) provide clarity for businesses in determining whether they are subject to the cybersecurity audit requirements and focus on personal information. In addition, the regulations already provide clarity regarding the extent to which the CCPA

		hand, another comment suggests changing the processed personal information amount from 250,000 to 500,000 and the processed sensitive personal information amount from 50,000 to 250,000. One comment suggests that the Agency clarify if these thresholds apply only to processing outside the context of an insurance transaction.	applies to insurance companies. (*See* § 7271(a).) The Agency does not believe that further clarification is necessary at this time. Further, comment does not provide any information as to why the proposed changes are more effective or appropriate than those adopted by the Agency.
7120	271	Comment argues that the text creates cybersecurity audit obligations that are broader than other industry standard cyber audits and asserts that the regulation should be revised to align with the activities defined as presenting a significant risk in Article 10, § 7150.	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to complete an annual cybersecurity audit, with the regulations establishing a process to ensure that audits are thorough and independent. The listed components in § 7123(c), are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. The CCPA requires the Agency to consider the size and complexity of the business, and the nature and scope of its processing activities, in determining whether a business's processing of consumers' personal information presents significant risk to consumers' security. (Civ. Code § 1798.185(a)(14)(A).) The criteria in § 7120(b) provide clarity for businesses in determining whether they are subject to the cybersecurity audit requirements and focus on personal information because their processing of personal information. Businesses whose processing of personal information meets the criteria present significant risk to consumers' security.
7120	853	Comment believes this section promotes clarity and guidance regarding which businesses must perform cybersecurity audits while considering the complexity of the	The Agency agrees with this comment, to the extent that it supports the Agency's regulations, and notes comment's support.

		business and nature and scope of its processing activities. Leveraging the gross revenue threshold from the statute benefits businesses because it reduces complexity by utilizing thresholds with which businesses are familiar and have already considered and analyzed.	
7120	1513	Comment argues that the term "audit" in § 7120 needs further definition to prevent confusion among professionals. Comment proposes distinguishing between different types of assurance services (e.g., financial audits vs. attestation engagements) and recommends aligning terminology with AICPA standards.	The Agency disagrees with this comment. The regulations define "cybersecurity audit" and "cybersecurity audit report" in §§ 7001(j) and (*l*). The regulation is reasonably clear about the requirements for an audit and applies a performative standard that gives businesses flexibility to craft a method that best fits their businesses' operations. However, the Agency revised § 7122(a) to add examples of procedures and standards accepted in the profession of auditing, including those from AICPA.
7120	1815	Comment recommends removing circular language in sections that refer to the term that is being described in § 7120.	It is unclear what language this comment believes is circular and should be removed, and comment provides no suggested alternative language. The regulation is reasonably clear based on the plain meaning of the words and applicable definitions. The Agency believes that no further clarification is needed at this time.
7120(b)	175, 248, 612, 1059, 1166, 1827, 1882	Comment argues that the proposed cybersecurity audit requirements exceed the agency's statutory authority under Civil Code § 1798.185(a)(15), and the triggers for a cybersecurity audit are not tied to each of the statutorily mandated criteria. For example, the revenue threshold in § 7120(b)(2) simply restates the revenue threshold to qualify as a regulated business under §1798.140(d)(1)(A) of the statute. It is inconsistent with the statutory text to treat the bare minimum threshold for	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to complete an annual cybersecurity audit, with the regulations establishing a process to ensure that audits are thorough and independent. The CCPA requires the Agency to consider the size and complexity of the business, and the nature and scope of its processing activities, in determining whether a business's processing of consumers' personal information presents significant risk to consumers' security. (Civ. Code §

		being a regulated entity under the statute as also presenting a significant risk. None of the other criteria consider the size of the business, nor do they consider the complexity of the business or sufficiently consider the nature of the business's processing activity. Comment argues that § 7120(b) assumes all CCPA-covered businesses present a high security risk and imposes cybersecurity audit requirements on all businesses subject to the CCPA, even if their processing does not present significant risk to consumer privacy or security. This overbroad approach places an undue burden on businesses, requiring unnecessary audits regardless of actual risk. Comment suggests modifying § 7120(b) to clarify that only businesses meeting specific thresholds should be subject to the requirement. Comment requests that the rules be revised to clarify that a business need not perform a cybersecurity audit unless the size, complexity, nature, and scope of its processing activities each pose a significant risk to consumers' privacy and security. Comment asserts that the regulations should allow for risk-based differentiation. Another comment suggests that § 7120(b) be modified to state that the processing of consumers' personal information presents significant risk to consumers' security if it involves a loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or	1798.185(a)(14)(A).) § 7120(b)(1)—deriving 50 percent or more of annual revenues from selling or sharing consumers' personal information—reflects the nature and scope of a business's processing activities, and can be a proxy for the business's complexity. § 7120(b)(2)(a) and (b)—the revenue and personal-information processing thresholds—reflect the business's size and complexity and the nature and scope of its processing activities. Businesses whose processing of personal information meets the criteria present significant risk to consumers' security. The comment's suggestion that the revenue threshold in § 7120(b)(2) treats being a regulated entity as presenting significant risk appears to reflect the comment's interpretation of the regulation, which is inconsistent with the regulations' language: § 7120(b)(2) requires the business to meet the revenue threshold as well as one of the personal-information processing thresholds in (b)(2)(a) or (b). § 7120(b) does not require all businesses subject to CCPA to complete a cybersecurity audit; it requires only businesses that meet specific criteria to complete a cybersecurity audit. In addition, the Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The comment's suggestions would not provide sufficient clarity for businesses to determine whether they are subject to the cybersecurity auditing requirements, would seem to apply only to businesses currently experiencing the loss of confidentiality, integrity, or availability expected to have severe or catastrophic adverse effects, and would add consideration of organizational impacts not focused on personal information. In regard to businesses subject to the jurisdiction of federal prudential regulators, exempting financial institutions would be inconsistent with the CCPA, which instead includes a data-level exemption for information subject to the Gramm-Leach-Bliley Act and implementing regulations; it applies to

		individuals. Yet another comment argues that the cybersecurity audit thresholds in § 7120(b)(2) are overly broad due to triggering based on "processing" rather than "buying, selling, or sharing" personal information and recommends replacing the language with a cross reference to Civil Code § 1798.140. Another comment suggests a provision indicating that the processing of consumer's personal information presents a significant risk to consumers' security if the business is not subject to examination or supervision by a federal prudential regulator.	"businesses" and does not exempt financial institutions. (*See* Civ. Code §§ 1798.140(d), 1798.145(e).)
7121	1158	Comment suggests adjusting the timing requirements for cybersecurity audits to align with those of other states, proposing an incident-based approach similar to risk assessments.	The Agency disagrees with this comment. Not requiring an annual thorough cybersecurity audit would be inconsistent with the CCPA, which requires the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to "perform a cybersecurity audit on an annual basis." (Civ. Code § 1798.185(a)(14)(A).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Nevertheless, the Agency has revised § 7121 to phase in implementation by annual gross revenue over a three-year period, provide additional time after the cybersecurity audit period to complete the cybersecurity audit report, clarify the audit coverage period, and clarify the specific date by which a business must complete its cybersecurity audit report.
7121	1419	Comment requests that the Agency include a provision that states that the cybersecurity audit must only take into account activities 24 months after the effective date of these regulations.	The Agency disagrees with this comment. The Agency has revised § 7121 to phase in implementation by annual gross revenue over a three-year period, provide additional time after audit period to complete the cybersecurity audit report, clarify the audit coverage period, and clarify the specific date by which a business must complete its cybersecurity audit report.

DRAFT

7121(a)	854	Comment appreciates the CPPA's recognition that businesses will need sufficient time to establish processes and implement procedures to conduct the cybersecurity audits contemplated by the regulations. Comment also indicates that this section also promotes clarity and eliminates doubt by specifying when the first audit must be conducted.	The Agency agrees with this comment to the extent that to the extent that it supports the Agency's regulations and notes comment's support.
7121(b)	193, 197, 646, 647, 710, 737, 879, 911, 919	Comment states that this should be removed, as it is unnecessarily burdensome to require businesses to repeat the lengthy process without any significant changes in their practices, and there is no tangible benefit to consumers from forcing businesses to repeat the same process they have already completed. Comment suggests if there is no material change, then the business should not be required to complete a cybersecurity audit with all the components of § 7123, but shall complete one at least once every three years. Comment suggests that the timing of audits should be risk based and consistent with global frameworks, like NIST and ISO 27001, which do not require annual audits. Another comment suggests revising the regulation to require business to complete their cybersecurity audits regularly, with once a calendar year as an example. Comment also suggests making conforming changes elsewhere where "annual" is referenced. Other comments indicate that the regulations do not account for business constraints or unforeseen circumstances;	The Agency disagrees in part with the comment. Not requiring an annual thorough cybersecurity audit would be inconsistent with the CCPA, which requires the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to "perform a cybersecurity audit on an annual basis," with the regulations establishing a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Nevertheless, the Agency has revised § 7121 to phase in implementation by annual gross revenue over a three-year period, provide additional time (approximately 90 days) after the cybersecurity audit period to complete the cybersecurity audit report, clarify the audit coverage period, and clarify the specific date by which a business must complete its cybersecurity audit report.

		regulations should allow for extension up to 90 days.	
7121(b)	794	Comment suggests that the regulations should be clarified as to whether businesses will have the ability to determine the scope of the subsequent audits or whether the audits must conform to the requirements set forth in Sections 7122(e) and 7123.	The Agency disagrees with this comment. The regulation is reasonably clear that each cybersecurity audit must meet the requirements set forth in Article 9, including § 7123(e), previously § 7122(e); and § 7123. The Agency believes that no further clarification is needed at this time.
7122	163, 199, 223 241, 242, 243, 244, 353, 389, 498, 529, 619, 621, 641, 642, 643, 738, 807, 861, 920, 1159, 1224, 1299, 1385, 1422, 1484, 1540, 1168, 1760, 1773, 1862, 1888	Comment recommends removing the requirements that internal auditors report to the business's board of directors, that cybersecurity audits and issues raised by them be reported to the business's board of directors, and that the business's board certify its review of the cybersecurity audit. Comment argues that the requirements for board involvement in cybersecurity audits are excessive, impractical, and inconsistent with standard corporate practices, as well as state, federal, and global standards. The board should not be required to sign off on audits, as this falls outside their traditional role. Instead, the responsibility should lie with the Chief Information Security Officer (CISO) or a comparable employee who has direct oversight of cybersecurity operations, or experts within the business. Comment also indicates that the Agency should clarify what must be reported to the business's board of directors or governing body. Comment suggests adding a statement that the audit committee or board shall be responsible for the effectiveness of internal audit systems and receive regular	The Agency agrees with this comment in part, to the extent that it recommends removing board-involvement requirements at this time. The Agency revised the regulations to remove board involvement requirements, which will simplify implementation at this time. § 7122(f), previously § 7122(h), no longer requires that the cybersecurity audit report be reported to the board, and instead allows it to be provided to a member of the business's executive management team who has direct responsibility for the cybersecurity program. Additionally, the Agency revised § 7122(a)(3) to remove requirements for board involvement and instead allow a member of the business's executive management team who does not have direct responsibility for the cybersecurity program to fulfill those requirements. Further, the Agency deleted § 7122(i), which removes the requirement for a board member to certify that the business has not attempted to influence the auditor's assessment and that the signer understands the audit findings, and revised § 7124(c) to remove the requirement for board-involvement and instead allow a member of the business's executive management team to fulfill the certification of completion requirements. The Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example.

		reports about audit issues. Comment further indicates that existing business management structures and board oversight should not be negatively impacted by the cybersecurity audit requirements or other cybersecurity frameworks and audits should be leveraged for flexibility.	The regulations implement the requirements of California law, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements.
7122	352, 398, 739, 740	Comment argues that many requirements in § 7122 conflict with existing federal cybersecurity requirements and guidelines. Specific problematic requirements include: mandatory board oversight of auditors, employee training after every data breach, and other prescriptive rules that do not align with federal financial institution standards. Comment recommends a more flexible approach that aligns with federal standards, such as the NIST Cybersecurity Framework, international frameworks, and existing requirements for federally regulated financial institutions. § 7122(e) should also be harmonized with existing audit requirements and standards.	The Agency disagrees with this comment. The CCPA makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196.) Additionally, the Agency has determined the regulations are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. Additionally, the Agency revised the regulations to remove requirements for board involvement and allow a member of the business's executive management team who does not have direct responsibility for the cybersecurity program to fulfill those requirements.
7122	1814	Comment recommends that thoroughness and independence of audits be split into separate sections to ensure both are treated as equally important responsibilities.	The Agency disagrees with this comment. The regulation is reasonably clear based on the plain meaning of the words, and the Agency believes that no further clarification is needed at this time. The comment's suggestion is not more effective or appropriate than the Agency's regulation.
7122(a)	1904	Comment supports the requirement for independent cybersecurity audits in § 7122 but argues that allowing internal auditors undermines the goal of true independence.	The Agency disagrees with this comment. § 7122 provides clarity and guidance regarding auditor objectivity and independence and is consistent with practices in the current

		Comment suggests the following language be added to § 7122: "The auditor must be fully independent, neither party to nor controlled by any party to any past or current relationship with the business apart from the provision of security auditing services."	marketplace in other contexts. It balances providing privacy protections for consumers and flexibility for businesses.
7122(a)	77, 78, 163, 620	Comment states that while the regulations allow for internal auditors, the independence requirements may force businesses to use external auditors. The unclear language on auditor independence could prohibit standard internal audit structures, restrict necessary interactions between auditors and senior management, and prevent auditors from making valuable cybersecurity recommendations, even though they lack authority to make implement the recommendation. Additionally, the limited availability of external auditors presents a serious compliance challenge.	The Agency disagrees with this comment. The regulations specifically permit the use of internal auditors. Additionally, the Agency revised § 7122(a)(3) to remove requirements for board involvement and allow 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 also added the phrase "if any" to clarify that businesses are not required to conduct performance evaluations of their auditors. The Agency also revised § 7122(a)(2), previously § 7122(a)(1), to clarify that an auditor may make recommendations regarding the business's cybersecurity program as part of articulating audit findings. The comment has provided no information to support that the availability of external auditors presents a serious compliance challenge; however, businesses can address this by using an internal auditor.
7122(a)	1514, 1515	Comment recommends establishing clearer and stricter standards for what constitutes a "qualified, objective, independent professional" under § 7122. They caution that differing interpretations of independence could create inconsistencies. Comment urges that the regulations require the use of recognized assurance standards, such as AICPA's attestation standards, in compliance with §7122. Comment argues that existing CPA standards offer a framework for independence,	The Agency disagrees with this comment. However, the Agency revised § 7122(a)(1) to clarify what it means to be a qualified auditor. The Agency also revised § 7122(a) to add examples of procedures and standards accepted in the profession of auditing, including those from AICPA. The CCPA directs the Agency to establish a process to ensure that audits are independent. (Civ. Code § 1798.185(a)(14)(A).) The requirements in § 7122 establish a process to ensure that audits are independent, provide clarity and guidance for businesses, and are consistent with approaches to independence taken in the current marketplace in other contexts.

		competence, and ethics, bringing credibility and consistency to audits. Comment provides System & Organization Controls (SOC) and SOC 2 for Cybersecurity reports as examples of frameworks.	
7122(a)(2) [previously 7122(a)(1)]	1885	Comment believes that this subsection is likely beyond the auditors' role to make "decisions" about the audit and/or the business being audited. Comment recommends deleting "decisions and."	The Agency disagrees with this comment, because being free to make decisions related to the audit without influence by the business is part of auditor independence. The comment's suggestion is not more effective or appropriate than the Agency's regulation.
7122(b)	1042	Comment argues that the regulations do not explicitly protect privileged information from being disclosed to auditors, raising confidentiality concerns. Comment requests an explicit clarification that businesses are not required to disclose information protected by attorney-client privilege or other evidentiary privileges.	The Agency disagrees with this comment. Explicit protection for privileged information is not necessary, because the regulations do not specifically require the provision of attorney-client privileged information.
7122(d)	984	Comment suggests that cybersecurity audits should rely on specific evidence rather than business attestations. To improve the readability of § 7122(d), comment suggests separating the text into two paragraphs.	The Agency agrees with this comment in part. The regulations require that no cybersecurity audit finding could rely primarily on attestations by business's management and must instead rely primarily upon specific evidence the auditor deems appropriate. Nevertheless, the Agency revised § 7122, to remove provisions that specify the content of the cybersecurity audit report and instead include a cross reference to where the Agency relocated those provisions. § 7122(d) as revised now addresses only what cybersecurity audit findings can rely upon.
7122(e)	231, 644, 862, 1825	Comment suggests revising § 7122(e) as follows: (e) The cybersecurity audit must: (1) Inventory, document, and summarize each applicable component of the business's	The Agency disagrees with this comment. The comment's suggestion is not more effective or appropriate than the Agency's regulation. Additionally, the Agency revised the regulations to move provisions specifying the content of a

		cybersecurity program set forth in § 7123; (2) Specifically identify any non-compliance with the business's documented cybersecurity program; (3) Specifically include identified issues related to the cybersecurity program from audits performed within the last 36 months and have not been resolved. Comment also recommends clarifying that the cybersecurity audit must specifically identify any material gaps or weaknesses in the business's cybersecurity program. Comment argues that without a materiality qualifier, audits could identify insignificant issues, such as an internet connection being a potential weakness, even when safeguarded with firewalls or VPNs.	cybersecurity audit from § 7122 to § 7123(e). § 7123(e)(3) also requires the cybersecurity audit to identify and describe in detail the status of any gaps or weaknesses of the policies and procedures in §7123(b)(1), the applicable components in § 7123(c), and any additional component assessed in accordance with § 7123(d) 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. The requirement in § 7123(e)(3) already covers gaps or weaknesses identified by previous audits that have not yet been resolved. This revision provides clarity for businesses and their auditors regarding the types of gaps or weaknesses that must be identified and described in the cybersecurity audit report.
7122(e)	645	Comment suggests that adding a "material" standard aligns the regulation with statutory language that focuses on significant risks to consumer privacy and security.	The Agency disagrees with this comment. The CCPA directs the Agency to require businesses whose processing of consumers' personal information presents significant risk to consumers' security to perform an annual cybersecurity audit. (Civ. Code § 1798.185(a)(14)(A).) That statutory language does not support adding a "material" standard, which would not provide sufficient clarity for businesses.
7122(e)(3)	1817	Comment suggests specifying the timeframe for which results from prior cybersecurity audits need to be included to provide clear expectations for both the business and the auditor.	The Agency disagrees with this comment. The Agency revised the regulations to delete § 7122(e)(3). The Agency also revised § 7123(e)(5), previously § 7122(e)(4), to require instead require that the report must identify any corrections or amendments to prior cybersecurity audit reports. The Agency believes that no further clarification is needed at this time.
7122(f) [previously 7122(h)]	1887	Comment recommends replacing "reported" with "provided" and argues that requiring a presentation of audit findings to the board may	The Agency agrees with the comment's recommendation and revised § 7122(f), previously § 7122(h), to replace "reported" with "provided." The Agency disagrees with this comment to the extent that it suggests that the regulations as initially

		exceed the board's mandate and is not within the Agency's authority to require.	proposed exceeded the Agency's authority. The regulations, including as initially proposed, are within the Agency's authority and are consistent with the CCPA's direction to the Agency to establish a process to ensure that audits are thorough and independent and to further the intent and purpose of the CCPA to protect consumers' privacy. (*See* Civ. Code § 1798.185(a)(14)(A); Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3.)
7122(g) [previously 7122(j)]	1423, 1620, 1672,	Comment supports the five-year retention requirement for cybersecurity audit data but expresses concern about the risks posed by prolonged storage of sensitive audit records. These records, if compromised, could expose detailed information about a business's potential vulnerabilities. Comment recommends that the regulations be expanded to include security safeguards for auditors who retain such data, specifying the controls that must be in place during and after an audit. Another comment raises concerns regarding a 5-year retention period and the lack of clarity on external auditor retention rules. Comment requests more flexibility and clearer standards for internal and external auditors. While another comment requests the retention period be revised to two years.	The Agency agrees with this comment's support for the retention requirement contained in § 7122(g), previously § 7122(j). However, the CCPA already requires businesses to implement reasonable security procedures and practices, and requires them to contractually require their service providers and contractors to provide the same level of privacy protection. (*See* Civ. Code §§ 1798.100(e), (d)(2).) The Agency has revised § 7122(g), previously § 7122(j), to clarify that the requirement to retain documents relevant to each cybersecurity audit applies to both the business and the auditor. The Agency believes that no further clarification is needed at this time. In regard to the retention period, the CCPA provides the Agency with five years to bring an administrative action alleging a violation of its provisions. Making the retention requirement consistent with the time period to bring an action ensures that relevant information would be available to the Agency and the business to determine if a violation occurred. The five-year period will also enable the business and its successive auditors to obtain information from prior audits, which is necessary to identify corrections or amendments to prior audits. (*See* § 7123(e)(5).)
7123	349, 354, 355, 387, 397, 399, 613, 741, 863, 892,	Comment argues that these requirements exceed the Agency's authority. The CCPA only mandates "reasonable security procedures and practices", and the Agency lacks authority to create broad cybersecurity mandates.	The Agency disagrees with this comment. The CCPA directs the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The regulations are consistent with this direction and do not require businesses

	912, 1024, 1033, 1200, 1247, 1300, 1315, 1424, 1527, 1621, 1788	Comment also asserts that the CCPA only authorizes the Agency to define audit scope, not to impose specific security measures. Comment suggests that the regulations improperly introduce new cybersecurity mandates under the audit framework, and that Civil Code § 1798.81.5 already governs security for certain businesses, exempting federally regulated financial institutions. Comment also asserts that such prescriptive regulations fail to account for different industries, the evolving cybersecurity landscape, will rapidly become obsolete, and the effort to avoid duplicative audits is practically unworkable. This could divert resources from real security improvements. Comment advocates aligning audit requirements with federal and global standards, such as NIST CSF, ISO 27001, SEC's cybersecurity disclosure rules, and GDPR security requirements. Comment also asserts that there are internal inconsistencies in the regulation, such as assessing both passwords and Zero Trust Architecture, which eliminates passwords. Comment further asserts that the regulations should be risk-based and aligned with federal frameworks. Comment suggests that the regulations include language that specifically allows businesses to meet the audit requirements by completing an audit using a recognized framework such as ISO 27001, SOC 2, NIST CSF, or a comparable standard, which includes not requiring submission of annual audits. Finally, comment indicates that businesses should be assured	to implement certain cybersecurity protections or practices. Rather, they provide clarity about how businesses must perform a thorough and independent cybersecurity audit. However, the Agency revised § 7123(c), previously § 7123(b)(2), to further clarify that the audit must assess listed components of a cybersecurity program that the auditor deems applicable to the business's information system. Additionally, exempting financial institutions would be inconsistent with the CCPA, which instead includes a data-level exemption for information subject to the Gramm-Leach-Bliley Act and implementing regulations; it applies to "businesses" and does not exempt financial institutions. (*See* Civ. Code §§ 1798.140(d), 1798.145(e).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The Agency used its discretion to adopt requirements appropriate to California. The regulations draw from and harmonize with existing frameworks and standards to the extent that doing so is consistent with the CCPA. The regulations implement the requirements of California law, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements. Nevertheless, the Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example to provide further guidance to businesses. Moreover, the Agency does not require the submission of an annual audit, but rather a certificate of completion. (*See* § 7124.) The Agency will continue to monitor the marketplace as cybersecurity practices evolve, to determine whether modifications to the regulations are necessary.

		that audit reports will remain confidential and that sensitive security details will not be disclosed.	
7123	351, 497, 622, 1350	Comment believes that the requirement for annual comprehensive cybersecurity audits is too burdensome, costly — particularly for small businesses — and may lead to inefficiencies. The annual requirement is too frequent when compared to other privacy laws. Comment asserts that nothing mandates the annual audits be of the same size and scope each year. Comment recommends a three-year audit cycle, with annual risk-based audits or assessments, would provide a more effective and flexible compliance structure, while being consistent with CCPA's direction to consider the "size and complexity of the business" and the "nature and scope of processing activities".	The Agency disagrees with this comment. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The majority of the costs of the regulations fall on larger businesses dealing with large amount of personal information and with annual revenues that are greater than $28 million. Nevertheless, the Agency has modified the regulations to significantly reduce the costs of the regulations on small businesses. Additionally, not requiring an annual thorough cybersecurity audit would be inconsistent with the CCPA, which requires the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to "perform a cybersecurity audit on an annual basis." (Civ. Code § 1798.185(a)(14)(A).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. At this time, the Agency has determined that audits of differing size and scope each year would not meet the CCPA requirement.
7123	695	Comment calls for cybersecurity audits to include connected vehicles as well as traditional IT systems. It also recommends following NIST 800-88 Rev. 1 guidelines for proper data disposal.	The Agency agrees with this comment to the extent that it supports the Agency's regulations. The regulations apply to connected vehicles and traditional IT systems to the extent that they are part of a business's "information system" and therefore subject to the business's cybersecurity program. The regulations are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses.
7123	1698	Comment suggests that the Agency include a data minimization component in § 7123. A cybersecurity audit should identify, assess, and document how the business's data	The Agency agrees with the comment's support for data-minimization. However, the regulations already include a component that addresses businesses' retention schedules and proper disposal of personal information. (*See* § 7123(c)(16),

		minimization program protects personal information from unauthorized access, destruction, use, modification, and disclosure. The business should maintain a data handling program to retain personal information for only as long as is reasonably necessary to fulfill the purpose for which it was collected, like what was required of Marriot/Starwood by an FTC consent agreement. Data minimization is the surest way to protect consumers' personal information.	previously § 7123(b)(2)(P).) The regulations also include requirements that the cybersecurity audit assess the business's establishment, implementation, and maintenance of its cybersecurity program; the components in § 7123(c) that the auditor deems applicable to the business's information system; and how the business implements and enforces compliance with them. (*See* § 7123(b).) Further, the Agency revised the regulations to clarify that nothing in § 7123 prohibits an audit from assessing and documenting components of a cybersecurity program that are not set forth in § 7123 (b) or (c). (*See* § 7123(d).)
7123(a) & (b)	194, 1826	Comment suggests revising § 7123(a) and (b) as follows: (a) The cybersecurity audit must measure and report compliance of the business' documented cybersecurity program. (b) The cybersecurity audit must specifically identify, document and assess. Comment also asserts that this audit should be able to be conducted using multiple audits, provided that all the requirements are satisfied across the multiple audits.	The Agency disagrees in part with this comment. However, the Agency revised the regulations to move provisions specifying the content of a cybersecurity audit from § 7122 to § 7123(e). The regulations already require a business's cybersecurity audit to describe how the business enforces compliance with, and to explain the effectiveness of, the policies and procedures in § 7123(b)(1), the applicable components in § 7123(c), and any additional component assessed in accordance with § 7123(d). (*See* § 7123(e)(2), previously § 7123(b)(3) and (c)(1).) The Agency also revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example to provide further guidance to businesses, which could utilize information from multiple audits to meet the regulations' requirements.
7123(b)(1)	1426	Comment requests deletion of "taking into account the state of the art and cost of implementing the components of a cybersecurity audit."	The Agency disagrees with this comment. The description of a business's cybersecurity program as "appropriate to the business's size and complexity and the nature and scope of its processing activities, taking into account the state of the art and cost of implementing the components of a cybersecurity program" is consistent with cybersecurity requirements and

			guidance in other contexts. The comment has not provided any information as to why their proposed change is more effective or appropriate than the regulations adopted by the Agency.
7123(b)(1), (c)(3)(D) [previously 7123(b)(2)(D)(iv)]	915	Comment argues that §§ 7123(b)(1) and 7123(b)(2)(D)(iv) are inconsistent regarding implementation versus enforcement of security programs.	The Agency disagrees with this comment. § 7123(b)(1) and § 7123(c)(3)(D), previously § 7123(b)(2)(D)(iv), implement the requirements of California law, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements.
7123(b)(2)(C)	235, 1034, 1160, 1214	Comment suggests that there are aspects of the cybersecurity audit regulations that require further clarification or could be less prescriptive to allow for differing but rigorous approaches to cybersecurity management. In particular, § 7123 requires an audit of the "Zero trust architecture," which could encompass many different things. The Agency's clarity on the intent and expectations for this particular section of the audit would be especially helpful. Comment also recommends modifying §7123(b)(2)(C) to state: "Zero trust architecture or least privileged access." Comment indicates zero trust architecture is too new and onerous to be required at this time.	The Agency disagrees with this comment. The Agency deleted § 7123(b)(2)(C), which addressed zero-trust architecture, to simplify implementation at this time. § 7123(c)(3)(a), previously § 7123(b)(2)(D), already addresses the concept of least-privileged access and provides examples of restricting each person's, account's, or application's privileges and access to personal information to what is necessary for that person, account, or application to perform their duties.
7123(b)(2), (c) [previously 7123(b)(2)]	639, 1348, 1573	Comment argues that § 7123(b) sets forth forty-four different criteria that a company must either implement or explain why it does not implement, which is prescriptive and exceeds this Agency's statutory authority. Comment asserts that in its granular list of activities that must be considered for cybersecurity audits, the Agency inappropriately creates broad cybersecurity governance requirements, such as password	The Agency disagrees with this comment. The CCPA directs the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The regulations are consistent with this direction and do not require businesses to implement certain cybersecurity protections or practices. Rather, they provide clarity about how businesses must perform a thorough and independent cybersecurity audit. Nevertheless, the Agency revised § 7123(c), previously § 7123(b)(2), to further clarify that the audit must assess listed

		protocols, cybersecurity training, and penetration testing, many of which will grow stale as best practices evolve. Comment also indicates that requiring a business to explain why alternative technology or processes to multi-factor authentication provide 'equivalent' security misses the point.	components of a cybersecurity program that the auditor deems applicable to the business's information system, and 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, to simplify implementation at this time. The regulations implement the requirements of California law, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements. The Agency will continue to monitor the marketplace as cybersecurity practices evolve, to determine whether modifications to the regulations are necessary.
7123(b)(3)	196	Comment suggests revising as follows: "For each of the applicable components set forth in subsections (b)(1)–(2), including the safeguards the business identifies in its policies and procedures, the cybersecurity audit must describe how the business implements and enforces compliance with them. This description may be either general or specific to each of the requirements."	The Agency disagrees with this comment. However, the Agency revised § 7123(e)(2), previously § 7123(c)(1), to incorporate the requirement from previous § 7123(b)(3). Specifically, § 7123(e)(2) now requires that the audit report describe how the business implements and enforces compliance with the policies and procedures identified in the regulation, the applicable components, and any additional component assessed. § 7123(e)(2) gives businesses flexibility in describing how they implement and enforce compliance.
7123(c) [previously 7123(b)(2)]	195, 913, 1776	Comment argues that the Agency should not require businesses to justify the use of compensating controls. If any justification for using compensating controls remains, it should include a materiality qualifier that requires explanations only for "materials gaps and weaknesses." In contrast, another comment suggests revising the regulation to include that the business must address the components of the business's cybersecurity program, as applicable and appropriate to the business's size and the complexity, nature, and scope of	The Agency disagrees with this comment. However, the Agency revised § 7123(c), previously § 7123(b)(2), to further clarify that the audit must assess listed components of a cybersecurity program that the auditor deems applicable to the business's information system. 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, to simplify implementation at this time. Additionally, § 7123(b)(1) already incorporates the concept that a business's cybersecurity program is appropriate to the business's size and complexity and the nature and scope of its

		its processing activities. If not applicable, the cybersecurity audit must document and explain any comparable components relevant to the business's protection of personal information. The comment also suggests that Agency should revise them to be more general and thus more future proofed. For example, the requirement in § 7123(b)(2)(A) should be limited to "authentication" as opposed to specific mechanisms for authentication (e.g., strong unique passwords which are already becoming out-of-date). Comment also asserts that the Agency should allow for zero trust or hybrid zero trust architecture and remove the encryption requirement.	processing activities. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. Nevertheless, the Agency deleted § 7123(b)(2)(C), which addressed zero-trust architecture, to simplify implementation at this time. The Agency believes that leaving the components as drafted provides greater clarity to businesses than providing more generalized components. The Agency will continue to monitor the marketplace as cybersecurity practices evolve, to determine whether modifications to the regulations are necessary.
7123(c) [previously 7123(b)(2)]	855	Comment supports the flexibility permitted in this section. Additionally, this aligns with the GLBA Safeguards Rule which requires an information security program "appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."	The Agency agrees with this comment to the extent that it supports the Agency's regulations and notes the comment's support.
7123(c) [previously 7123(b)(2)]	1039, 1060, 1316, 1485, 1573, 1775, 1829	Comment suggests striking cybersecurity program components in § 7123(b)(2). This list of components does not constitute a risk-based approach that allows businesses to appropriately tailor their implementation of these audits to the size and complexity of their operations, including the nature and scope of processing activities and expectations of their customers. It is simply a list of current cybersecurity technologies and is overly prescriptive, while running the risk of quickly	The Agency disagrees with this comment. § 7123(b)(1) already incorporates the concept that a business's cybersecurity program is "appropriate to the business's size and complexity and the nature and scope of its processing activities. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. However, although the Agency strives for alignment with other privacy and security laws and existing standards when appropriate, it must comply with California law

		becoming outdated. Most existing cybersecurity audit standards call for the assessment of how organizations achieve outcomes (e.g., NIST recommends as a security control, "The confidentiality, integrity, and availability of data-at-rest are protected."). The regulations instead require specific security controls to achieve certain outcomes (e.g., requiring assessment of "Encryption of personal information, at rest"). For example, (b)(2)(A) focuses on MFA and passwords when most companies are increasingly moving to passkeys. Comment asserts that §7123(b)(2) imposes cybersecurity requirements that do not align with recognized frameworks like NIST CSF, ISO 27001, and SOC-2.	and use its discretion to adopt requirements appropriate to California. The Agency revised § 7123(c)(1)(B), previously § 7123(b)(2)(A)(i), to add language clarifying that the subsection would be applicable only if the business uses passwords or passphrases. Strong unique passwords are an example of authentication. Additionally, the Agency deleted § 7123(b)(2)(C), which addressed zero-trust architecture, to simplify implementation at this time. The Agency will continue to monitor the marketplace as cybersecurity practices evolve, to determine whether modifications to the regulations are necessary.
7123(b) & (c)	1425	Comment requests that the Agency add language indicating the provisions apply only to the processing of personal information.	The Agency disagrees with this comment. However, the Agency revised the definition of "information system" to further focus on "personal information," while retaining that an information system includes resources "that can provide access to personal information." (§ 7001(t).) The Agency also revised § 7123(c), previously § 7123(b)(2), to further clarify that the audit must assess listed components of a cybersecurity program "that the auditor deems applicable to the business's information system."
7123(c) [previously 7123(b)(2)]	232, 856	Comment states that the text introduces uncertainty as it does not specify when multi-factor authentication is required (i.e., when accessing any information system). The text does define "information system" in § 7001(v). Accordingly, comment suggests adding "for any individual accessing any information system;" in the end of the section. Comment	The Agency disagrees with this comment. However, the Agency revised § 7123(c), previously § 7123(b)(2), to further clarify that the audit must assess listed components of a cybersecurity program that the auditor deems applicable to the business's information system. The regulation is reasonably clear based on the plain meaning of the words and the context in which they are used. The Agency believes that no further clarification is needed at this time. Additionally, § 7123(c)(1), previously §

		suggests modifying § 7123(b)(2)(A)(i) to focus on phishing resistant authentication mechanisms, regardless of whether the mechanism requires single or multi-factor authentication.	7123(b)(2)(A), already addresses authentication more broadly, and the inclusion of "multi-factor authentication that is resistant to phishing attacks" in § 7123(c)(1)(A), previously § 7123(b)(2)(A)(i), does not preclude an audit from assessing a business's use of other means of phishing-resistant authentication. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses.
7123(c) [previously 7123(b)(2)]	233, 914, 985	Comment recommends removing § 7123(b)(2)(A)(ii), regarding strong unique passwords or pass phrases, as these are easily phished or stored in unsecured databases. Comment argues that § 7123(b)(2)(A)(ii) requires password security assessment, which conflicts with § 7123(b)(2)(C). Comment suggests that cybersecurity audit regulations should reference evolving industry standards, like NIST, to ensure password and access control policies remain relevant.	The Agency disagrees with this comment. The Agency has determined that the regulations are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. The Agency revised § 7123(c)(1)(B), previously § 7123(b)(2)(A)(i), to add language clarifying that the subsection would be applicable only if the business uses passwords or passphrases. The cybersecurity audit regulations do not require businesses to implement certain cybersecurity protections or practices. Additionally, zero-trust architecture does not conflict with the use of strong unique passwords. Nevertheless, the Agency deleted § 7123(b)(2)(C), which addressed zero-trust architecture, to simplify implementation at this time. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. Referencing evolving standards as suggested would not provide sufficient clarity to business regarding their obligations under the regulation. The Agency will continue to monitor the marketplace as cybersecurity practices evolve, to

			determine whether modifications to the regulations are necessary.
7123(c) [previously 7123(b)(2)]	1349	Comment indicates the prescriptive list of "components" contradicts applicable California law and offers no flexibility to focus on components that are appropriate for the processing activity, underlying data, or business's environment. It only offers that compensating controls "provide at least equivalent security." California law and industry best practices incorporate a risk-based approach based on reasonableness. Existing security standards and frameworks already exist, so the regulations do not need to create a new set of components to be evaluated. The ISOR does not provide a rationale for why these expert-driven, multi-stakeholder, and regularly updated standards and frameworks are not sufficient to address significant risks to consumer security. The regulations should permit businesses flexibility to address topics most appropriate for the processing activity, including by reference to existing standards and frameworks. Comment also suggests revising § 7122(e) and § 7123(c) to say "may" and include the terms "material" gaps or weaknesses.	The Agency disagrees with this comment. However, the Agency revised § 7123(c), previously § 7123(b)(2), to further clarify that the audit must assess listed components of a cybersecurity program that the auditor deems applicable to the business's information system. The Agency has 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, to simplify implementation at this time. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. The Agency believes that leaving the components as drafted provides greater clarity to businesses than providing more generalized components. The Agency will continue to monitor the marketplace as cybersecurity practices evolve, to determine whether modifications to the regulations are necessary.
7123(c)(2) [previously 7123(b)(2)(B)]	1038	Comment argues that § 7123(b)(2)(B) requiring an auditor to consider "[e]ncryption of personal information, at rest and in transit" is too vague and open-ended to be useful. Leaving which method of encryption is appropriate unanswered could lead some businesses to	The Agency disagrees with this comment. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. The Agency does not believe that

		potentially perform encryption that is expensive but not a meaningful defense against reasonably anticipated threats. Comment requests that the Agency revise this section to reference other well-established standards for encrypting information of this type with a preference for NIST standards if possible.	referencing external encryption standards would answer the question of which encryption method would be appropriate in a given information system and factual situation. The regulations are meant to apply to many factual situations and across industries, and to be robust yet flexible to account for differences among businesses and their information systems. The Agency has determined that no further clarification is needed at this time.
7123(c) [previously 7123(b)(2)]	857, 858	Comment believes that although these components are similar to those included in other frameworks, they deviate from the language of those frameworks. This increases the cost and complexity of compliance for businesses which will be required to parse the language and determine if the requirements are different and more expansive than existing frameworks. The Agency's imposition of different requirements is largely duplicative of existing security standards and increases compliance burdens without materially advancing cybersecurity protections. To ensure consistency and standardization, comment recommends the Agency mirror the language of the GLBA Safeguards Rule in its outline of cybersecurity program components. Comment suggests adding "over external networks" to the end of § 7123(b)(2)(B)'s "encryption of personal information, at rest and in transit."	The Agency disagrees with this comment. Although the Agency strives for consistency with privacy laws in other jurisdictions when appropriate, it must comply with California law and use its discretion to adopt requirements appropriate to California. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. However, the Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example. The comment's suggestion to add "over external networks" is unnecessary, because the Agency revised § 7123(b)(2) to clarify that the cybersecurity audit must assess the listed components of a business's cybersecurity program "that the auditor deems applicable to the business's information system," and the Agency revised the definition of "information system" to clarify that it includes "the resources organized for the business's processing of personal information, regardless of whether the business owns those resources." Therefore, a business's "information system" already includes "external networks" organized for the

			processing of personal information, and the business's cybersecurity audit must assess the encryption component if the auditor deems it applicable to the business's information system.
7123(c)(2) [previously 7123(b)(2)(B)]	234	Comment recommends modifying §7123(b)(2)(B) to state: "Encryption of personal and sensitive information, at rest and in transit."	The Agency disagrees with this comment. § 7123(c)(2), previously § 7123(b)(2)(B), addresses "personal information," which already includes sensitive personal information. Sensitive information that is not personal information is not subject to the CCPA.
7123(c)(3)(A) [previously 7123(b)(2)(D)(i)]	986	Comment proposes revising the requirements for access control within § 7123(b)(2)(D). This addresses various facets of access control, including employee access, management of privileged accounts, account creation monitoring, and physical access controls. Comment recommends revisions to enhance specificity, enforce best practices, dynamic adjustments based on job duties, and align with international standards as demonstrated in the NIS2 Directive and learned from the California Attorney General's recent Blackbaud enforcement action. The language can be more precise by referring to a "user" or an "account" instead of a "person" when referencing account and access controls. Many accounts on modern systems do not belong to a single person but are associated with a system or application that is credentialed to access and process data.	The Agency agrees in part with this comment and has revised § 7123(c)(3)(A), previously § 7123(b)(2)(D)(i), to add "account's, or application's" for clarity when privileges or access is not granted to an individual person. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses.
7123(c)(4)(B) [previously	1035	Comment believes that "allowlisting" is not commonly used outside high-security environments.	The cybersecurity regulations do not require businesses to implement certain cybersecurity protections or practices. Rather, they provide clarity about how businesses must perform a thorough and independent cybersecurity audit. After

7123(b)(2)(E)(ii)]			again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. The regulations include "allowlisting" as an example of how businesses inventory and manage personal information and their information system. Additionally, the Agency revised § 7123(c), previously § 7123(b)(2), to further clarify that the audit must assess listed components of a cybersecurity program "that the auditor deems applicable to the business's information system." The regulations are meant to apply to many factual situations and across industries, and to be robust yet flexible to account for differences among businesses and their information systems.
Previous 7123(c)(5)	245	Comment recommends modifying § 7123(c)(5) to state: Include the date that the cybersecurity program and any evaluations thereof were presented to the business's highest-ranking executive of the business responsible for the business's cybersecurity program. Comment recommends removing 7123(c)(5) because the requirement to include a date that the "cybersecurity program and any evaluations thereof were presented" is unnecessary and excessive. Comment argues that the term "cybersecurity program" is not defined and the business should not be required to present the cybersecurity program and evaluations to the board of directors.	The Agency disagrees with this comment. However, the Agency deleted § 7123(c)(5) to simplify implementation at this time. Additionally, the regulations define "cybersecurity program" in § 7001(k), previously § 7001(m).
7123(c), (c)(5) [previously	356	Comment states that many listed cybersecurity requirements, including § 7123(b)(2)(F), appear to include requirements that extend beyond personal data protection, potentially	The Agency disagrees with this comment. Whether a business's cybersecurity audit would be enterprise-wide or narrower would depend upon the business's enterprise and how the business set up its information system. However, the Agency

7123(b)(2), (b)(2)(F)]		necessitating an enterprise-wide assessment. The Agency should clarify that these requirements apply only when personal data is involved.	revised the definition of "information system" to further focus on "personal information," while retaining that an information system includes resources "that can provide access to personal information." The Agency also revised § 7123(c), previously § 7123(b)(2), to further clarify that the audit must assess listed components of a cybersecurity program "that the auditor deems applicable to the business's information system." Therefore, § 7123(c)(5), previously § 7123(b)(2)(F), pertains to the secure configuration of hardware and software within the business's information system, and the business's information system is focused on personal information.
7123(c)(6) [previously 7123(b)(2)(G)]	236	Comment recommends modifying § 7123(b)(2)(G) to state: "Internal and external vulnerability scans, penetration testing, and disclosure and reporting on patched and exploitable vulnerabilities," deleting "(e.g., bug bounty and ethical hacking programs)."	The Agency disagrees with this comment. The disclosure and reporting referenced in § 7123(c)(6), previously § 7123(b)(2)(G), should not be limited to patched and exploited vulnerabilities. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. The examples of bug-bounty and ethical hacking programs provide clarity and guidance for businesses and auditors about how businesses often implement vulnerability disclosure and reporting activities.
7123(c)(7) [previously 7123(b)(2)(H)]	237	Comment recommends modifying § 7123(b)(2)(H) to state: "Audit-log management."	The Agency disagrees with this comment. Maintaining the phrase "including the centralized storage, retention, and monitoring of logs" in § 7123(c)(7), previously § 7123(b)(2)(H), provides clarity for businesses and auditors about how businesses often implement audit-log management.
7123(c)(8)(A) [previously	1037	Comment states that the requirements for Bot-Detection are neither specific enough nor narrowly tailored to the goal. This language could be improved by explicitly stating the	The Agency agrees with this comment in part and has revised § 7123(c)(8)(A), previously § 7123(b)(2)(I), to clarify that a business may use technologies such as bot-detection, intrusion-detection, and intrusion-prevention "to detect unsuccessful login attempts, monitor the activity of authorized

7123(b)(2)(I)]		goals of these security technologies in the main text rather than in an example.	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."
7123(c)(9) [previously 7123(b)(2)(J)]	238	Comment recommends modifying §7123(b)(2)(J), regarding antivirus and anti-malware protections to focus on endpoint detection and response (EDR) mechanisms.	The Agency disagrees with this comment. An audit's assessment of antivirus and antimalware protections does not need to focus on endpoint protection and response mechanisms. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses.
7123(c)(10) [previously 7123(b)(2)(K)]	239	Comment recommends removing § 7123(b)(2)(K), as segmentation of information is primarily achieved at the network level and would be accounted for under § 7123(b)(2)(I), regarding network monitoring and defenses.	The Agency disagrees with this comment. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. The inclusion of segmentation and examples provide clarity and guidance for businesses and auditors about how businesses often implement network segmentation.
7123(c)(11) [previously 7123(b)(2)(L)]	1427	Comment requests that this subsection deleted.	The Agency disagrees with this comment. Retaining "limitation and control of ports, services, and protocols" in § 7123(c)(11), previously § 7123(b)(2)(L), is consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses.
7123(c)(12) & (13) [previously 7123(b)(2)(M)]	1040, 1428	Comment finds (ii) "how the business maintains current knowledge of changing cybersecurity threats and countermeasures" inconsistent and confusing. It appears unrelated to the first one, as well as cybersecurity awareness, education	The Agency agrees with this comment in part and has revised §§ 7123(c)(12) and (13), previously § 7123(b)(2)(M), to make the subsections easier to read, and to address cybersecurity awareness separately from cybersecurity education and training. However, the descriptions of cybersecurity awareness,

		and training generally. Comment inquires if businesses are expected to perform cybersecurity awareness, education and/or training on how they maintain knowledge of current and evolving cybersecurity threats. Comment requests that it be removed so that the training subsection is cohesive, and that "including" as well as subsections (i) and (ii) be deleted.	education, and training in §§ 7123(c)(12) and (13), previously § 7123(b)(2)(M), provide clarity for businesses and auditors about how businesses maintain knowledge of changing threats and countermeasures, and how and when they implement education and training.
7123(c)(14) [previously 7123(b)(2)(N)]	1161	Comment requests clarification on which entities should be responsible for identifying and documenting cybersecurity practices, such as secure development and coding, particularly in relation to developers of AI systems.	The Agency disagrees with this comment. The regulations require a "business" that meets the criteria set forth in § 7120(b) to complete a cybersecurity audit. The Agency revised § 7123(c), previously § 7123(b)(2), to further clarify that the audit must assess the listed components of a cybersecurity program "that the auditor deems applicable to the business's information system." The listed components include secure development and coding. The Agency believes that no further clarification is needed at this time.
7123(c)(15) [previously 7123(b)(2)(O)]	1429	Comment recommends deleting this subsection.	The Agency disagrees with this comment. The Agency has not deleted § 7123(c)(15), previously § 7123(b)(2)(O). Oversight of service providers, contractors, and third parties is an important part of protecting consumers' security and is consistent with other cybersecurity frameworks.
7123(c)(16) [previously 7123(b)(2)(P)]	1430	Comment requests that the Agency delete how businesses are to properly dispose of personal information.	The Agency disagrees with this comment. The Agency has not deleted § 7123(c)(16), previously § 7123(b)(2)(P). The descriptions of disposal methods provide clarity and guidance for businesses and auditors about how businesses often properly dispose of personal information no longer required to be maintained.
7123(c), (c)(17) [previously	357, 615, 640, 865,	Comment asserts that the definition of "security incident" is overly broad, exceeds the Agency's authority, is inconsistent with	The Agency disagrees with this comment. The CCPA directs the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough. (Civ.

7123(b)(2), (b)(2)(Q)(i)]	1347, 1372	California's cybersecurity breach laws, and deviates from federal standards. The regulations should incorporate the definition of security incident that already exists in California's s data breach notification statute and require the provision of prior security incident notifications only when the business was required to notify a California regulator. The audit should not include all notifications provided to any domestic or global regulator regarding a security incident even if it does not affect the personal information of California consumers. Comment argues that the inclusion of the phrase "or potentially" creates an issue of overbreadth, and the phrase "…or availability of a business's information systems or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of the business's cybersecurity program" not only requires compliance for a threat and not an actual incident, but also expands regulation to all businesses' information systems regardless of whether they are associated in any way with consumer personal information. Audits should assess response processes rather than analyze every potential unauthorized occurrence. Alternately, the Agency can consider focusing on unauthorized access or compromise of critical systems and data that impact personal information.	Code § 1798.185(a)(14)(A).) The Agency determined that unauthorized access to consumers' personal information that were significant enough to trigger notifications to other agencies or data processing authorities are relevant to assessing a business's cybersecurity posture. However, the Agency revised § 7123(e)(10), previously § 7123(e), to remove language regarding notifications to other agencies or data processing authorities outside of California to simplify implementation at this time. Additionally, the Agency revised the definition of "security incident" in § 7123(c)(17), previously § 7123(b)(2)(Q)(i), to replace "potentially" with "imminently," to simplify implementation at this time; and to add "personal" to focus on personal information. The Agency disagrees with the comment's suggestion to use California's breach-notification statute, which defines "personal information" more narrowly and does not define "security incident." The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. § 7123(c)(17), previously § 7123(b)(2)(Q), already addresses a business's incident-response processes and does not require an auditor to analyze every security incident. In addition, the Agency revised the definition of "information system" to further focus on "personal information," while retaining that an information system includes resources "that can provide access to personal information." The Agency also revised § 7123(c), previously § 7123(b)(2), to further clarify that the audit must assess listed components of a cybersecurity program "that the auditor deems applicable to the business's information system." Therefore, the listed components in § 7123(c), previously § 7123(b)(2), pertain to the business's information system, and the business's information system is focused on personal information. Although the Agency strives for alignment with other privacy and security laws and existing standards when

			appropriate, it must comply with California law and use its discretion to adopt requirements appropriate to California.
7123(c)(17) [previously 7123(b)(2)(Q)]	1431	Comment requests that the Agency change "i.e." to "e.g." and include in the cybersecurity audit only the information about the business's documentation of predetermined instructions to detect, respond to, limit, and recover from a security incident.	The Agency disagrees with this comment. The use of "i.e." is appropriate, because it clarifies that how the business manages its responses to security incidents is, in other words, its incident response management. In addition, a cybersecurity audit should not be limited to assessing the business's documentation and should include how the business tests its incident-response capabilities.
7123(d) [previously 7123(b)(4)]	1169	Comment suggests that the cybersecurity audit requirements should align with existing industry standards such as NIST or ISO 27001. The open-ended audit scope in § 7123(b)(4) should be revised to avoid ambiguity and ensure audits remain manageable and effective.	The Agency disagrees with this comment. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. The provision does not require businesses to assess components outside of those required; however, including this language provides clarity to businesses. The Agency does not believe that further clarification is necessary at this time.
7123(e)(3) & (4) [previously 7123(c)(2) & (3)]	616, 864, 1828	Comment raises a concern that the inclusion of detailed descriptions of a company's security weaknesses, such as weaknesses in multi-factor authentication, intrusion detection, and other defensive systems, could become roadmaps to bypassing a company's cybersecurity defenses and would therefore pose risk to consumers' security. Comment asserts that businesses need discretion to use compensating controls without triggering additional auditing requirements. Comment also suggests striking § 7123(c)(3) requirements for businesses to document	The Agency disagrees with this comment. The CCPA directs the Agency to establish a process to ensure that audits are thorough and to define the scope of the audit. (Civ. Code § 1798.185(a)(14)(A).) Requiring the cybersecurity audit to include the gaps and weaknesses in a business's cybersecurity program is part of ensuring that the audit is thorough and is consistent with Civ. Code § 1798.185(a)(14)(A). However, the Agency revised § 7123(c), previously § 7123(b)(2), including to delete 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, to simplify implementation at this time.

DRAFT

		security gaps identified in audits, which could expose them to legal risks in case of a breach.	
7123(e)(4) [previously 7123(c)(3)]	1036	Comment states that a resolution timeframe is a reasonable expectation, but audit plans and management action plans in response to them do not typically contain resource allocations. This requirement is not a standard audit practice and, in light of how typical audits operate, comment requests the Agency remove the phrase "the resources it has allocated to resolve them and" from § 7123(c)(3).	The Agency disagrees with this comment. However, the Agency revised § 7123(e)(4), previously § 7123(c)(3), to remove "resources it has allocated to resolve them," to simplify implementation at this time.
7123(e)(6) [previously 7123(c)(4)]	358, 866, 917, 1886	Comment suggests that the audit requirements should focus on key cybersecurity personnel rather than listing all contributors. Comment also asserts that only the titles of employees in senior roles of responsibility for the cybersecurity program should be required. Comment asserts that the information necessary to provide accountability within the business should be left up to the business itself to determine and, as the name and titles of the individuals do not aid anyone outside the business in this understanding, this requirement is unnecessary; thus requires the collection, use and retention of extraneous personal information of these individuals.	The Agency agrees with this comment in part and accordingly revised § 7123(e)(6), previously § 7123(c)(4), to clarify that a business is not required to provide more than three titles of qualified individuals responsible for the business's cybersecurity audit program. This provides flexibility for businesses that have many individuals responsible for their cybersecurity programs. The Agency has determined that in order to ensure accountability and to aid in future audits or necessary investigations, this information is necessary; it does not implicate extraneous personal information.
7123(e)(8) [previously 7122(g)]	1420, 1421	Comment requests for it to be optional to include a statement that is signed and dated by each auditor that certifies that the auditor completed and independent review. Comment also requests the Agency to make it optional to	The Agency disagrees with this comment. The CCPA directs the Agency to establish a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The Agency determined that requiring the auditor to certify the independence of their audit is relevant to the thoroughness and independence of a cybersecurity audit. However, the

		include the auditor's name, affiliation, and relevant qualifications.	Agency revised § 7123(e)(8), previously § 7122(g), to apply the certification requirement only to the highest-ranking auditor, to simplify implementation at this time and provide flexibility for different businesses models. The Agency determined that the auditor's name, affiliation, and relevant qualifications are relevant to the thoroughness and independence of a cybersecurity audit.
7123(e)(9) [previously 7123(d)]	867, 918	Comment argues that § 7123(d) creates redundancy by requiring businesses to submit breach notifications already reported under California law. Comment asserts that this should be removed or substantially narrowed.	The Agency disagrees with this comment. The CCPA directs the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough. (Civ. Code § 1798.185(a)(14)(A).) The Agency determined that unauthorized access to consumers' personal information that were significant enough to trigger notifications to consumers are relevant to assessing a business's cybersecurity posture.
7123(e)(9) & (10) [previously 7123(d) & (e)]	400	Comment suggests that §§ 7123(d)-(e) require national banks to report data breaches to state regulators violate federal visitorial rights, which limit state oversight of national banks. Additionally, such disclosures could increase cybersecurity risks by exposing sensitive information without significant benefits.	The Agency disagrees with this comment. The CCPA makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196.) Moreover, the CCPA includes a data-level exemption for information subject to the Gramm-Leach-Bliley Act and implementing regulations, but the CCPA applies "businesses" and does not exempt financial institutions. (*See* Civ. Code §§ 1798.140(d), 1798.145(e).) Regarding "disclosures" increasing cybersecurity risks, the comment's interpretation of the regulations appears to be inconsistent with the regulations' language, which requires a business to submit a certification of completion to the Agency, not its cybersecurity audit report. (*See* § 7124.) The Agency is also required to comply with the Information Practices Act of 1977. (*See* Civ. Code §§ 1798–1798.78.)
7123(e)(9) & (10) [previously	742, 797	Comment argues that the language would require businesses to provide notifications or notice of compliance to state regulators,	The Agency agrees with this comment's observation that the regulations would require a business to provide information about notifications provided to consumers or to other agencies

7123(d) & (e)]		including information about data breaches and copies of breach notification letters. Comment is concerned this requirement is overly burdensome and may be duplicative.	or data processing authorities. The CCPA directs the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough. (Civ. Code § 1798.185(a)(14)(A).) The Agency determined that unauthorized access to consumers' personal information that were significant enough to trigger notifications to other agencies or data processing authorities are relevant to assessing a business's cybersecurity posture. However, the Agency revised § 7123(e)(10), previously § 7123(e), to remove language regarding notifications to other agencies or data processing authorities outside of California to simplify implementation at this time. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA.
7123(e)(10) [previously 7123(e)]	359, 617, 868, 908, 1041, 1279, 1301, 1884	Comment states that § 7123(e) would require businesses operating in California to report breaches occurring anywhere in the world, even if they are outside the Agency's jurisdiction. Comment asserts that this is an unjustified expansion of state authority. Comment suggests striking the provision. Another comment suggests adding "the same or similar incidents could reasonably be expected to impact consumers" and argues they should only be required to include incidents that could reasonably affect California consumers. Comment indicates that this subsection should be consistent with § 7123(e)(9). Additionally, comment asserts that cybersecurity auditors lack the expertise to analyze such notices. Additionally, disclosing detailed security information could inadvertently provide attackers with insights into corporate vulnerabilities, increasing future risks. Instead of imposing broad and redundant	The Agency disagrees with this comment. The CCPA directs the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough. (Civ. Code § 1798.185(a)(14)(A).) The Agency determined that unauthorized access to consumers' personal information that were significant enough to trigger notifications to other agencies or data processing authorities are relevant to assessing a business's cybersecurity posture. However, the Agency revised § 7123(e)(10), previously § 7123(e), to remove language regarding notifications to other agencies or data processing authorities outside of California to simplify implementation at this time. Regarding "disclosures" increasing cybersecurity risks, the comment's interpretation of the regulations appears to be inconsistent with the regulations' language, which requires a business to submit a certification of completion to the Agency, not its cybersecurity audit report. (*See* § 7124.) The Agency is also required to comply with the Information Practices Act of 1977. (*See* Civ. Code §§ 1798–1798.78.)

		reporting mandates, the Agency should focus on CCPA-specific requirements and issue guidance on how it will safeguard reported security information.	
7123(f)	1883	Comment agrees with the Agency's reasoning in the ISOR, and suggests that this subsection appear at the beginning of § 7123.	The Agency notes comment's support. However, the regulation is reasonably clear, and the comment's suggestion does not provide additional clarity, nor is more effective or appropriate than the Agency's regulation.
7123(f)	124, 240, 360, 387, 401, 618, 623, 743, 797, 916, 1094, 1099, 1277, 1380, 1572, 1673	Comment criticizes the audit requirements outlined in § 7123(f) for being too rigid and disconnected from other standard cybersecurity practices. Comment argues that the requirement under § 7123(f) that businesses must supplement pre-existing cybersecurity audits, assessments, or certifications if they do not fully align with California's standards is unnecessarily burdensome, duplicative, and costly. Comment asserts that requiring proof that all audit elements were considered, undermines usefulness of using another audit and that the Agency allow more flexibility. Comment argues that businesses that already have to complete similar audits for other business purposes, would now have to meet all the requirements of the regulations, driving up costs and resources to change auditing practices. Comment asserts that no other audit regime looks like the Agency audit, so businesses will always have to conduct a separate audit for compliance with the audit provisions. California should allow businesses to comply by using existing federal or globally recognized	The Agency disagrees in part with this comment. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. Nevertheless, the Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example. The Agency also removed the requirement that a business specifically explain how the cybersecurity assessment work it is utilizing meets the requirements set forth in the regulations, to simplify implementation at this time. To the extent the comment suggests that the Agency should accept a business's use of a cybersecurity audit framework in lieu of meeting the cybersecurity audit requirements in Article 9, the Agency disagrees with that suggestion, because a business's use of another framework does not ensure that the business conducted a thorough and independent cybersecurity audit focused on securing consumers' personal information. The regulations implement the requirements of California law, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements.

		cybersecurity frameworks instead. Comment requests the Agency include in the regulation a list of other frameworks that will be accepted as compliant.	
7123(f)	387	Comment recognizes that many businesses already comply with cybersecurity audits, but argues that the Agency is overstepping its authority by imposing detailed cybersecurity requirements rather than just audits.	The Agency disagrees with this comment. The CCPA directs the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The regulations are consistent with this direction and do not require businesses to implement certain cybersecurity protections or practices. Rather, they provide clarity and guidance about how businesses must perform a thorough and independent cybersecurity audit.
7123(f)	435, 2033	Comment asserts that overreaching regulations will stifle innovation, divert critical resources from lifesaving research, put California's life sciences companies at a competitive disadvantage globally, and disproportionately impact smaller businesses, without delivering meaningful consumer privacy benefits. Life science companies already conduct rigorous cybersecurity audits under federal regulations, and these audits cover things like encryption and access controls. The Agency should allow existing frameworks to avoid duplication without compromising security.	The Agency disagrees with this comment. The CCPA includes certain data-level exemptions but applies to "businesses." (*See* Civ. Code §§ 1798.140(d), 1798.145(c), 1798.146(a)(1), (4), and (5).) The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security to perform an annual cybersecurity audit, and establishing a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Although the Agency strives for alignment with other privacy and security laws when appropriate, it must comply with California law and use its discretion to adopt requirements appropriate to California. However, the Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA, and has modified

			the regulations to significantly reduce the costs of the regulations on small businesses, and to simplify implementation for businesses at this time.
7124	1100	Comment argues that requiring businesses to submit cybersecurity audit certifications contradicts California Civil Code § 1798.185(14), which only requires risk assessments to be submitted, not audits. Comment requests that § 7124 be deleted.	The Agency disagrees with this comment. § 7124 is consistent with the CCPA's direction to the Agency to establish a process to ensure that audits are thorough and independent and to further the intent and purpose of the CCPA to protect consumers' privacy. (*See* Civ. Code § 1798.185(a)(14)(A); Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3.)
7124	1486	Comment recommends including language in § 7124 to allow businesses that engage in alternate cybersecurity audits, assessments, or evaluations that meet this Article's requirements to submit substitute documentation in lieu of annual certificates of completion, the validity period of which will be recognized accordingly. This will reduce the regulatory burden on such businesses.	The Agency disagrees with this comment. The Agency determined that the certification of completion requirements are relevant to the thoroughness and independence of the audit and therefore included the requirements. However, the Agency revised § 7124 to clarify the information that the certification must include. The Agency also revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example.
7124	1890	Comment recommends removing § 7124 entirely. Comment argues that Civil Code § 1798.185(a)(15)(A) specifies only that the Agency must issue regulations requiring businesses to perform cybersecurity audits on an annual basis. Requiring businesses to annually certify completion of a cybersecurity audit will become a burdensome, check-the-box task that increases costs without improving consumer privacy or security. It also claims that the CPRA does not authorize the Agency to mandate such certifications except outside of an investigation. Moreover, the ISOR's explanation that certification is	The Agency disagrees with this comment. § 7124 is consistent with the CCPA's direction to the Agency to establish a process to ensure that audits are thorough and independent and to further the intent and purpose of the CCPA to protect consumers' privacy. (*See* Civ. Code § 1798.185(a)(14)(A); Prop. 24, as approved by voters, Gen. Elec. (Nov. 3, 2020), § 3.) Annual certifications to the FTC and annual notices to the Superintendent of the New York Department of Financial Services did inform the certification requirement in the regulations.

		"informed by practices in other contexts, such as FTC orders" is not on point.	
7124(c)	246, 1888	Comment recommends replacing certification by a member of the board or governing body with certification by the highest-ranking executive with authority to certify on behalf of the business and who is responsible for oversight of the business's cybersecurity-audit compliance. Comment argues that the requirement that a business's board "sign off" on the audit findings with the required statement may exceed the authority of some boards as it is more of an operational requirement.	The Agency agrees with this comment in part. The Agency revised § 7124(c) to clarify who must complete the certification and replaced the requirement that it be a member of the board or governing body, with a requirement that it be a member of the business's executive management team who (1) is directly responsible for the business's cybersecurity-audit compliance; (2) has sufficient knowledge of the business's cybersecurity audit to provide accurate information; and (3) has the authority to submit the business's certification to the Agency.
7124(c)	921, 1317, 1574	Comment suggests that § 7124(c) and related provisions should clarify that only a certificate of completion is shared with the Agency, not the full audit report. Comment also suggests that language be included that states that a business is not required to disclose trade secrets or other security information. Comment further indicates, if more disclosure is required, safeguards should prevent public release, keeping the confidential under FOIA requests and protect trade secrets.	The Agency disagrees with this comment. The regulations are already clear that a business must submit a certification of completion to the Agency, not its cybersecurity audit report. Additionally, providing disclosures to the Agency does not equate to it being disclosed; whether information in the Agency's records is subject to public disclosure depends on the specific information and whether an exception to the PRA applies. The Agency is also required to comply with the Information Practices Act of 1977. (*See* Civ. Code §§ 1798–1798.78.)
7124(c) & (d) [previously 7124(b) & (c)]	1162	Comment asks for more details on the certification submission process, such as who can submit the certification and the format in which it should be submitted, to ensure clarity and reduce the risk of noncompliance.	The Agency agrees with this comment in part, and has revised § 7124 to clarify who must submit the certification, the criteria they must meet, and the information the certification must include.

7124(c) & (d) [previously 7124(c)]	1433	Comment requests that § 7124(c) be deleted.	The Agency disagrees with this comment. However, the Agency revised § 7124(c) to clarify who must complete the certification and replaced the requirement that it be a member of the board or governing body, with a requirement that it be a member of the business's executive management team who (1) is directly responsible for the business's cybersecurity-audit compliance; (2) has sufficient knowledge of the business's cybersecurity audit to provide accurate information; and (3) has the authority to submit the business's certification to the Agency. The Agency also added § 7124(d), which requires that the certification be signed and include the date of the certification.
7124(d)(3) [previously 7124(b)]	1432	Comment requests that the requirement to identify the 12 months that the audit covers is deleted.	The Agency disagrees with this comment. The CCPA directs the Agency to establish a process to ensure that audits are thorough. (Civ. Code § 1798.185(a)(14)(A).) The Agency determined that the time period covered by an audit is relevant to the thoroughness of the audit and therefore included the requirement. Nevertheless, the Agency revised § 7124 to clarify the information that the certification must include, and moved the requirement to § 7124(d)(3), previously § 7124(b).
CS Audits	141, 198	Comment suggests adding a provision that deems businesses in full compliance with Article 9 if it completes a cybersecurity audit, assessment, or evaluation that complies with the requirements of the Federal Financial Institutions Examination Council's IT Examination Handbook, the Gramm-Leach-Bliley Act, or the New York Department of Financial Services' Cybersecurity Regulation. Comment also urges the Agency to include a provision that deems the business in compliance with the cybersecurity audit provisions if it has conducted any audit, assessment, or evaluation conducted under the	The Agency disagrees with this comment. However, the Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example. The Agency also removed the requirement that a business specifically explain how the cybersecurity assessment work it is utilizing meets the requirements set forth in the regulations, to simplify implementation at this time. To the extent the comment suggests that the Agency should accept a business's use of a cybersecurity audit framework in lieu of meeting the cybersecurity audit requirements in Article 9, the Agency disagrees with that suggestion, because a business's use of another framework does not ensure that the

		National Institute of Standards and Technology's ("NIST") Cybersecurity Framework and successor frameworks released by NIST, the Cyber Risk Institute Profile and successor frameworks, or by or under the supervision of federal prudential regulators. This will avoid duplication and redundancy.	business conducted a thorough and independent cybersecurity audit focused on securing consumers' personal information. The regulations implement the requirements of California law, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements.
CS Audits	161, 388, 528, 566, 1483	Comment raises concerns the cybersecurity audit regulations exceed the Agency's jurisdiction. For example, the regulations include specific technical controls and frameworks that businesses must implement, effectively dictating operational security measures. The insurance and financial services sectors already follow industry-leading cybersecurity frameworks and standards such as NIST, the NAIC Insurance Data Security Model Law, and the New York Department of Financial Services Cybersecurity Regulation, which are comprehensive and evolve with emerging threats. Additionally, comment argues that other cybersecurity audits already performed by businesses (e.g., ISO 27001 and SOC 2 audits) should satisfy CCPA requirements, and allow use of internal and external auditors. Comment further argues the regulations duplicate existing federal regulations (such as HIPAA and FDA guidelines), increasing costs unnecessarily.	The Agency disagrees with this comment. The regulations are within the Agency's delegated authority under the CCPA. (*See* Civ. Code § 1798.185(a)(14)(A).) The CCPA directs the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough and independent. (Id.) The regulations are consistent with this direction and do not require businesses to implement certain cybersecurity protections or practices. Rather, they provide clarity and guidance about how businesses must perform a thorough and independent cybersecurity audit. However, the Agency revised § 7123(c), previously § 7123(b)(2), to further clarify that the audit must assess listed components of a cybersecurity program that the auditor deems applicable to the business's information system. In addition, the regulations focus on personal information as defined under the CCPA, and do not impose requirements on information that is subject to an exemption under the CCPA, such as those for FCRA and GLBA. The CCPA makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196. Although the Agency strives for alignment with other laws, the Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The Agency must comply with California law and use its discretion to adopt requirements appropriate to California. The regulations are already clear that

			a business may use internal or external auditors. (*See* § 7122(a)(2).) In addition, the Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example. To the extent the comment suggests that the Agency should accept a business's use of a cybersecurity audit framework in lieu of meeting the cybersecurity audit requirements in Article 9, the Agency disagrees with that suggestion, because a business's use of another framework does not ensure that the business conducted a thorough and independent cybersecurity audit focused on securing consumers' personal information. The regulations implement the requirements of California law, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements.
CS Audits	162, 223, 230, 247, 1058, 1774	Comment states that overly prescriptive cybersecurity audit regulations conflict with established risk-based approaches used by financial institutions. Current frameworks allow organizations to tailor cybersecurity measures to their specific risk profiles and audit at different cadences, whereas the regulations impose a one-size-fits-all annual model. This could create inefficiencies, hinder adaptability to evolving threats, and lead to unnecessary compliance burdens. Rules should align with widely accepted frameworks such as NIST, CSF, ISO 27001, and SOC 2 Type 2, and should specify that audits under comparable industry frameworks and recognized standards meet the requirements of the audit provisions. Agency should moderate thresholds for when	The Agency disagrees with this comment. The regulations are within the Agency's delegated authority under the CCPA. (*See* Civ. Code § 1798.185(a)(14)(A).) The CCPA directs the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough and independent. (Id.) The regulations are consistent with this direction and do not require businesses to implement certain cybersecurity protections or practices. Rather, they provide clarity and guidance about how businesses must perform a thorough and independent cybersecurity audit. However, the Agency revised § 7123(c), previously § 7123(b)(2), to further clarify that the audit must assess listed components of a cybersecurity program that the auditor deems applicable to the business's information system. Additionally, the criteria in § 7120(b) provide clarity for businesses in determining whether they are subject to the cybersecurity audit requirements because their processing of personal information presents significant risk to consumers' security. The CCPA requires the Agency to

		an audit is required and require them only when there is a significant risk.	consider the size and complexity of the business, and the nature and scope of its processing activities, in determining whether a business's processing of consumers' personal information presents significant risk to consumers' security. Although the Agency strives for alignment with other laws, the Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The Agency must comply with California law and use its discretion to adopt requirements appropriate to California. The Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example. To the extent the comment suggests that the Agency should accept a business's use of a cybersecurity audit framework in lieu of meeting the cybersecurity audit requirements in Article 9, the Agency disagrees with that suggestion, because a business's use of another framework does not ensure that the business conducted a thorough and independent cybersecurity audit focused on securing consumers' personal information. The regulations implement the requirements of California law, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses.
CS Audits	223, 318	Comment argues that the regulations should define "qualified, objective, independent professionals" for cybersecurity audits and clarify the scope of "significant risk to consumers' security," which should be defined consistent with leading cybersecurity law.	The Agency disagrees with this comment. However, the Agency has revised § 7122(a)(1) to clarify what it means to be a qualified auditor. The thresholds in § 7120(b) already articulate when a business's processing of consumers' personal information presents significant risk to consumers' security, consistent with the CCPA's provision that the Agency establish

		Regulations should clarify whether business can rely on third-party audits to meet compliance requirements.	a process to ensure that audits are thorough while providing flexibility to businesses. The regulations draw from and harmonize with existing frameworks and standards to the extent that doing so is consistent with the CCPA. The regulations implement the requirements of California law, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements. The Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example.
CS Audits	348	Comment states that the cybersecurity audit requirements in Article 9 impose significant compliance burdens, particularly on small and medium-sized businesses. The regulations depart from existing cybersecurity frameworks without justification, and critics argue they should be harmonized with established standards like NIST.	The Agency disagrees with this comment. The CCPA requires the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to perform an annual cybersecurity audit, and establishing a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The Agency revised § 7123(c), previously § 7123(b)(2), to further clarify that the audit must assess listed components of a cybersecurity program "that the auditor deems applicable to the business's information system." The Agency has 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, to simplify implementation at this time. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the

			Agency establish a process to ensure that audits are thorough while providing flexibility to businesses.
CS Audits	391, 496	Comment raises concerns about cybersecurity audit requirements, arguing they could divert resources from improvements and hinder security efforts by misallocating resources toward compliance rather than threat prevention. Comment indicates they could disproportionately burden smaller businesses.	The Agency disagrees with this comment. The regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. In addition, most of the costs of the regulations fall on larger businesses dealing with large amount of personal information and with annual revenues that are greater than $28 million. Nevertheless, the Agency has modified the regulations to significantly reduce the costs of the regulations, including for small businesses.
CS Audits	571	Comment argues that the regulation fails to differentiate between cybersecurity audits and assessments, which could lead to ineffective compliance efforts. Comment explains that assessments measure effectiveness, while audits measure compliance against specific requirements. Comment urges the Agency to clarify this distinction to ensure businesses correctly implement security measures aligned with the intent of the regulation.	The Agency disagrees with this comment, because the regulations define "cybersecurity audit" and provide clarity about how businesses must perform a thorough and independent cybersecurity audit, consistent with the CCPA. (*See* Civ. Code § 1798.185(a)(14)(A).) The Agency does not believe that further clarification is necessary at this time.
CS Audits	614, 635	Comment states that the regulations contradict the White House's National Cybersecurity Strategy, which emphasizes a unified, coordinated approach that minimizes compliance costs and burdens. The Agency's approach would divert businesses' resources toward compliance instead of actual cybersecurity improvements.	The Agency disagrees with this comment. The regulations do not contradict the National Cybersecurity Strategy ("Strategy"), which directs federal, not state, regulatory agencies to "leverag[e] existing international standards in a manner consistent with current policy and law" and states that, "where feasible," regulators should work to harmonize regulations with the objective of supporting national security and public safety. Nevertheless, the regulations draw from and harmonize with existing frameworks and standards to the extent that doing so is consistent with the CCPA, which governs the Agency's regulatory authority.

CS Audits	634, 1830	Comment argues that the proposed rules fail to recognize widely accepted industry frameworks (e.g., NIST, ISO, PCI-DSS) or offer an effective safe harbor for businesses that have already conducted similar cybersecurity audits. Comment advocates for allowing businesses to rely on existing frameworks and recognizing audits that follow industry-standard frameworks, such as ISO/IEC 27000 and NIST, as sufficient to meet California's requirements.	The Agency disagrees with this comment. However, the Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example. The Agency also removed the requirement that a business specifically explain how the cybersecurity assessment work it is utilizing meets the requirements set forth in the regulations, to simplify implementation at this time. To the extent the comment suggests that the Agency should accept a business's use of a cybersecurity audit framework in lieu of meeting the cybersecurity audit requirements in Article 9, the Agency disagrees with that suggestion, because a business's use of another framework does not ensure that the business conducted a thorough and independent cybersecurity audit focused on securing consumers' personal information. The regulations implement the requirements of California law, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements.
CS Audits	636, 2010	Comment asserts that businesses which complete the cybersecurity audits should be deemed to have met the reasonable standard of care, thereby precluding a private right of action under the CCPA's personal data breach provision. The Agency should explicitly allow businesses that comply with the cybersecurity audit requirements to use them as an affirmative defense against liability. This approach aligns to the CCPA as mandate to uphold reasonable security and ensure that resources are directed where they matter most, protecting consumer data.	The Agency disagrees with this comment. The CCPA does not contain a provision that allows the Agency to create or preclude a private right of action, or determine if the business can use compliance with the regulations as an affirmative defense in litigation. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.

CS Audits	637	Comment argues that Article 9 exceeds the CPPA's statutory authority by broadly defining "significant risk" in a way that captures nearly all businesses	The Agency disagrees with this comment. § 7120(b) does not require all businesses subject to CCPA to complete a cybersecurity audit and has made efforts to limit the burden of the regulations while implementing the CCPA. The CCPA requires the Agency to consider the size and complexity of the business, and the nature and scope of its processing activities, in determining whether a business's processing of consumers' personal information presents significant risk to consumers' security. The criteria in § 7120(b) provide clarity for businesses in determining whether they are subject to the cybersecurity audit requirements and focus on personal information.
CS Audits	707	Comment contends that insurance companies already comply with rigorous cybersecurity laws, including the NAIC Insurance Data Security Model Law and New York Department of Financial Services (NYDFS) Cybersecurity Regulation. Comment argues that the cybersecurity requirements could create duplicative obligations, increasing compliance burdens without improving security. Instead, comment suggests harmonizing the regulations with existing frameworks to ensure consistency. Specifically, asserts the regulations should add a new § 7123(g) to specifically recognize reports and/or certifications as generally sufficient, not require board to certify audits, and remove the requirement that companies notify the Agency of every security incident. Comment indicates that the guiding principle should be that any cybersecurity audit should focus on risk rather than other factors such as arbitrary frequency of audits.	The Agency disagrees in part with this comment. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to complete an annual cybersecurity audit, with the regulations establishing a process to ensure that audits are thorough and independent. The CCPA requires the Agency to consider the size and complexity of the business, and the nature and scope of its processing activities, in determining whether a business's processing of consumers' personal information presents significant risk to consumers' security. (Civ. Code § 1798.185(a)(14)(A).) The Agency determined that businesses whose processing of personal information meets the criteria the criteria in § 7120(b) present significant risk to consumers' security. The listed components in § 7123(c) are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. However, the Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its

			own or through supplementation; the Agency has also included an example. To the extent the comment suggests that the Agency should accept a business's use of a cybersecurity audit framework in lieu of meeting the cybersecurity audit requirements in Article 9, the Agency disagrees with that suggestion, because a business's use of another framework does not ensure that the business conducted a thorough and independent cybersecurity audit focused on securing consumers' personal information. The regulations implement the requirements of California law, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements. In addition, the Agency revised § 7124(c) to clarify who must complete the certification and replaced the requirement that it be a member of the board or governing body, with a requirement that it be a member of the business's executive management team who (1) is directly responsible for the business's cybersecurity-audit compliance; (2) has sufficient knowledge of the business's cybersecurity audit to provide accurate information; and (3) has the authority to submit the business's certification to the Agency. Regarding notifications of security incidents, the comment's interpretation of the regulation appears to be inconsistent with the regulations' language as notification is not required for all incidents, and the regulations require a business to submit a certification of completion to the Agency, not its cybersecurity audit report. (*See* §§ 7123(e)(9), (10), 7124).) Finally, not requiring an annual thorough cybersecurity audit would be inconsistent with the CCPA, which requires the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to "perform a cybersecurity audit on an annual basis." (Civ. Code § 1798.185(a)(14)(A).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.

DRAFT

CS Audits	1199, 1541	Comment argues that the regulations impose burdensome compliance requirements without appropriate justification. The regulations provide no threshold to evaluate the significance of the risk of harm to consumers before imposing additional costly and burdensome cybersecurity requirements upon the organization. In contrast, comment indicates that basing thresholds solely on revenue and consumer data volume, fail to account for industry-specific risk differences. Comment further asserts that some businesses may face disproportionate compliance costs without meaningful security benefits.	The Agency disagrees with this comment. The criteria in § 7120(b) provide clarity for businesses in determining whether they are subject to the cybersecurity audit requirements and focus on personal information. The CCPA requires the Agency to consider the size and complexity of the business, and the nature and scope of its processing activities, in determining whether a business's processing of consumers' personal information presents significant risk to consumers' security. § 7120(b)(1)--deriving 50 percent or more of annual revenues from selling or sharing consumers' personal information--reflects the nature and scope of a business's processing activities, and can be a proxy for the business's complexity. § 7120(b)(2)(a) and (b)--the revenue and personal-information processing thresholds--reflect the business's size and complexity and the nature and scope of its processing activities. Businesses whose processing of personal information meets the criteria present significant risk to consumers' security. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA, and revised the regulations to reduce the costs for businesses at this time, while generating significant benefits for businesses and consumers, such as reducing the risk of costly incidents 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.
CS Audits	1213	Comment generally supports the cybersecurity audit provisions, particularly those based on widely accepted standards, such as multi-factor authentication, strong passwords, and encryption.	The Agency agrees with this comment and notes comment's support.

CS Audits	1266	Comment argues that while audits help organizations document cybersecurity measures, they only provide a point-in-time assessment rather than real-time security insights. Comment warns against over-reliance on audits for determining security posture.	The Agency agrees with the comment's warning against overreliance upon audits for determining cybersecurity posture and that audits provide a point-in-time assessment.
CS Audits	1265	Comment supports the Agency's goal of protecting businesses and citizens from cyber threats and promoting effective cybersecurity practices.	The Agency agrees with this comment and notes comment's support.
CS Audits	1267	Comment supports the inclusion of identity protection in the proposed regulation, emphasizing that authentication, account management, and access controls are essential components. The regulation's flexibility is beneficial, but organizations should go beyond the basic requirements.	The Agency agrees with this comment, to the extent it supports the protections in the cybersecurity audit regulations.
CS Audits	1269	Comment agrees with the Agency's emphasis on logging practices, which help organizations retain security-relevant log data for proactive security measures, threat hunting, and investigations. Next Generation Security Information and Event Management (Next-gen SIEM) solutions rely on such data to enhance cybersecurity outcomes.	The Agency agrees with this comment, to the extent it supports the protections in the cybersecurity audit regulations.
CS Audits	1270	Comment emphasizes the importance of proactive threat hunting as a critical cybersecurity measure that helps detect and neutralize threats that breach even well-defended enterprises. Comment asserts that effective threat hunting requires continuous monitoring, automation, and hypothesis-driven	The Agency agrees with and notes comment's support for businesses being proactive in identifying and neutralizing threats to consumers' privacy and security.

		detection methods. Comment concludes that it is closely linked to network monitoring, defense, and cybersecurity threat awareness components of the regulation.	
CS Audits	1271	Comment suggests including endpoint detection and response (EDR) solutions in the regulations, as they are critical for detecting and responding to threats across various endpoints, including desktops, cloud workloads, and mobile devices.	The Agency agrees with this comment to the extent that it supports proactive cybersecurity measures. The regulations are clear that an audit may assess components of a cybersecurity program that are not specifically set forth in § 7123(b) or (c). (*See* § 7123(d).) After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. The comment's suggestion is no more effective or appropriate than the regulation adopted by the Agency.
CS Audits	1280	Comment recommends that the Agency prioritize intelligence-sharing initiatives over excessive reporting obligations. Rather than requiring businesses to file duplicative reports, the comment asserts that the Agency should facilitate industry discussions, publish security bulletins, and encourage information sharing between regulated entities and government agencies. These measures would enable businesses to anticipate and mitigate cyber threats proactively while reducing unnecessary compliance burdens.	The Agency disagrees in part with this comment. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to perform a cybersecurity audit on an annual basis, with the regulations establishing a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. To the extent the comment suggests that the Agency should modify the regulations to add facilitation of industry discussions, publication of security bulletins, or encouragement of information sharing between businesses and government agencies, the Agency disagrees with this comment at this time. The regulations balance protections for consumer privacy and simplifying implementation for businesses at this time. The Agency will continue to monitor the marketplace as cybersecurity practices evolve, to

			determine whether modifications to the regulations are necessary.
CS Audits	1382	The cybersecurity audit reporting requirements are not only out-of-step with other state laws, but also conflict with widely accepted cybersecurity frameworks, standards, and controls, such as those set forth by NIST and ISO.	The Agency disagrees with this comment. The comment does not explain how the regulations are out of step with other state laws and does not articulate any conflict between the regulations and cybersecurity frameworks, standards, or controls. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses.
CS Audits	1384	The regulations impose burdensome and prescriptive cybersecurity reporting and audit requirements that run counter to federal frameworks, including the White House's National Cybersecurity Strategy and Office of the National Cyber Director, and are not required by other state privacy frameworks. The Agency should align the regulations with global and federal cybersecurity standards and frameworks, which foster a balanced, risk-based approach to cybersecurity governance. Congress has consistently reiterated the importance of harmonizing cybersecurity regulations for strengthening the nation's cybersecurity posture.	The Agency disagrees with this comment. The CCPA directs the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The regulations are consistent with this direction and do not require businesses to implement certain cybersecurity protections or practices. Rather, they provide clarity and guidance about how businesses must perform a thorough and independent cybersecurity audit. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. Although the Agency strives for consistency with privacy and security laws in other jurisdictions when appropriate, it must comply with California law and use its discretion to adopt requirements appropriate to California. The Agency revised § 7123(c), previously § 7123(b)(2), to further clarify that the audit must assess listed components of a cybersecurity program that the auditor deems applicable to the business's information system. The Agency has 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, to simplify implementation at this time.

			After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses.
CS Audits	1350	Comment supports the flexibility in allowing internal or external auditors and the 24-month compliance window but criticizes the lack of flexibility in audit content and process. Comment suggests that the regulations should provide clear direction on the high-level objectives for the cybersecurity audits and allow companies to implement existing standards and best practices to meet said objectives.	The Agency agrees with the comment's support for flexibility in the regulations regarding internal or external auditors and the time for businesses to come into compliance. The Agency modified § 7121 to phase in implementation by annual gross revenue over a three-year period. This will provide small businesses additional time to come into compliance. Regarding the content and process of the cybersecurity audit, the regulations are consistent with the CCPA's direction to the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) They provide clarity for businesses on how to complete an audit. To that end, the Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example. The regulations implement the requirements of California law, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements.
CS Audits	1400, 1512	Comment expresses concern with Article 9 of the regulations. Comment acknowledges the importance of cybersecurity audits but argues that the current audit requirements are vague and could hinder effective compliance. Additionally, comment asserts that the cybersecurity audit sections require subjective judgment of the auditor about the sufficiency	The Agency agrees with this comment to the extent that it supports the importance of cybersecurity audits. After consideration of comments, the Agency has added clarity to the provisions related to cybersecurity audits and made changes to simplify implementation for businesses at this time. This includes revising § 7122(a)(1) to clarify what it means to be a qualified auditor, and has revised § 7122(a) to add examples of procedures and standards to provide more clarity for

		of cybersecurity protocols. Because the regulations would not provide an auditor with sufficient clarity to understand how to conduct audits, they are unconstitutionally vague.	businesses and their auditors. The regulation is reasonably clear about the requirements for an audit and applies a performative standard that gives businesses flexibility.
CS Audits	1580	Comment recommends aligning technical terms and definitions with national and industry standards organizations, such as the National Institute of Standards and Technology (NIST).	The Agency agrees in part with this comment, to the extent it supports harmonization. The Agency disagrees with this comment, to the extent it argues that additional modifications to the regulations are necessary to enable harmonization. The regulations harmonize with other frameworks while furthering the intent and purposes of the CCPA and providing clarity to businesses regarding their obligations.
CS Audits	1619, 1994	Comment raises general concerns about audit frequency, cost of compliance, vague thresholds for significant risk, and a need for stronger confidentiality and redaction protections in audit submissions to avoid exposure of sensitive business information.	The Agency disagrees with this comment. Not requiring an annual thorough cybersecurity audit would be inconsistent with the CCPA, which requires the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to "perform a cybersecurity audit on an annual basis." (Civ. Code § 1798.185(a)(14)(A).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Additionally, the criteria in § 7120(b) provide clarity for businesses in determining whether they are subject to the cybersecurity audit requirements and focus on personal information. Moreover, the regulations require a business to submit a certification of completion to the Agency, not its cybersecurity audit report. (*See* § 7124.) It is important to note that providing disclosures to the Agency does not equate to it being exposed; whether information in the Agency's records is subject to public disclosure depends on the specific information and whether an exception to the PRA applies.
CS Audits	1697	Comment supports requiring a qualified, objective, and independent auditor because it ensures robust cybersecurity audits that will ultimately better protect the safety of	The Agency agrees with this comment to the extent that it supports the Agency's regulations and notes comment's support.

		Californians' personal information. Comment also supports requiring service providers and contractors to provide all relevant information to the business' auditor to complete the audit. This is a privacy-protective provision to encourage businesses to thoroughly vet their third-party affiliates and their data security practices.	
CS Audits	1651, 1655	Comment argues that the cybersecurity audit requirement would impose an unnecessary burden on service providers without providing demonstrable benefit to California businesses. The annual cybersecurity audit requirement is unworkable for service providers with large client bases. Comment asserts that providing standardized security documentation should be sufficient and avoids privacy risks from direct audits. Comment also asserts that the audit requirement would divert security staff from meaningful cybersecurity tasks to repetitive audit responses, reducing overall security effectiveness. In addition, the regulations lack exemptions for trade secrets or proprietary information, potentially deterring innovation and causing companies to be less forthcoming. Comment opposes the mandatory audit provision as overly burdensome, especially for large-scale service providers.	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to complete a thorough and independent cybersecurity audit annually. (Civ. Code § 1798.185(a)(14)(A).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The requirements regarding service providers only apply to the personal information the service provider collected pursuant to its written contract with the business, and the Agency has revised the regulations to clarify that this only includes information in the service provider's possession, custody, or control. (*See* § 7050(h)(1).) Further, providing disclosures to the Agency does not equate to the information being disclosed; whether information in the Agency's records is subject to public disclosure depends on the specific information and whether an exception to the PRA applies.
CS Audits	1694	Comment supports the cybersecurity audit requirements. Cybersecurity audits provide redress to security incidents and promote good security practices. They identify risks before they materialize against consumers and	The Agency agrees with this comment and notes comment's support.

		encourage businesses to invest in strong data security protections. Comment supports the framing of Article 9 to center on risk to consumers instead of merely risk to businesses.	
CS Audits	1696	The scope of the cybersecurity audit requirements ensure complete auditing. Comment supports the regulations and sees them as an example of the Agency leading the way to better protect the data security of consumers. They will prevent businesses from submitting a weaker or less complete audit because they are required to do so under a different law or regulation.	The Agency agrees with this comment and notes comment's support.
CS Audits	1744	Comment supports the cybersecurity audit proposal, commending that it's in line with best practices from agencies like NIST and CISA. They highlight the rules' flexibility for businesses already in compliance with other regimes, streamlined audit verification requirements, and the benefit of annual audits to evaluate and remediate cybersecurity hygiene on a regular basis.	The Agency agrees with this comment and notes comment's support.
CS Audits	1778, 1782, 1784, 1789	Comment states that drawing from NIST frameworks, a fundamental challenge with annual cybersecurity audits is their static nature, which is inadequate for evolving cybersecurity threat. Comment suggests that the Agency should require businesses to integrate automated cybersecurity governance tools and AI-driven compliance monitoring into Article 9 cybersecurity audits. This should include: continuous security posture	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations requiring businesses, whose processing of consumers' personal information presents significant risk to consumers' security, to perform a thorough and independent audit annually. (Civ. Code § 1798.185(a)(14)(A).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The regulations provide flexibility for businesses and do not require businesses to implement certain cybersecurity protections or practices, nor do they impose requirements regarding the means by

		evaluations, real-time AI model performance monitoring and risk assessments, automated control validation, continuous compliance automation, and real-time threat intelligence. By incorporating scalable, technology-driven approaches, businesses can enhance compliance, reduce regulatory burdens, streamline cybersecurity audits, enhance real-time risk monitoring, improve enforcement mechanisms, and ultimately strengthen consumer trust. Comment suggests that the incident response planning should be more explicitly aligned with real-time threat detection and intelligence-sharing frameworks.	which businesses implement cybersecurity protections or practices. Rather, the regulations provide performance standards for how to comply with the CCPA cybersecurity audit requirement. The Agency will continue to monitor the marketplace as cybersecurity practices evolve, to determine whether modifications to the regulations are necessary.
CS Audits	1783	Comment suggests greater clarity for third-party vendor risk management, including automated tracking of vendor security incidents, evaluation of open-source vulnerabilities, and real-time risk analysis of service providers.	The Agency disagrees with this comment. The regulations already include a component of oversight of service providers, contractors, and third parties. (*See* § 7123(c)(15).) Additionally, the regulations provide flexibility for businesses and do not require businesses to implement certain cybersecurity protections or practices, nor do they impose requirements regarding the means by which businesses implement cybersecurity protections or practices. Rather, the regulations provide performance standards for how to comply with the CCPA cybersecurity audit requirement.
CS Audits	1785	Comment suggests that as AI-driven authentication and security screening systems become more prevalent, it should be considered to integrate Non-Human Identity (NHI) governance frameworks into their cybersecurity audits to ensure that that businesses deploy AI-based identity verification tools capable of detecting	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations requiring businesses, whose processing of consumers' personal information presents significant risk to consumers' security, to perform a thorough and independent audit annually. (Civ. Code § 1798.185(a)(14)(A).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The regulations provide flexibility for businesses and do not require businesses to implement certain cybersecurity protections or practices,

		synthetic identities, biometric fraud, and algorithmic bias.	nor do they impose requirements regarding the means by which businesses implement cybersecurity protections or practices. Rather, the regulations provide performance standards for how to comply with the CCPA cybersecurity audit requirement. The Agency will continue to monitor the marketplace as cybersecurity practices evolve, to determine whether modifications to the regulations are necessary.
CS Audits	1786	Comment states that while Article 9 appropriately mandates encryption for data at rest and in transit, it does not explicitly address future-proofing data security against post-quantum cryptographic threats. They suggest the Agency include post-quantum encryption strategies and emphasize granular access controls like attribute-based access control (ABAC), just-in-time privileged access management (JIT-PAM), and zero-trust security models.	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations requiring businesses, whose processing of consumers' personal information presents significant risk to consumers' security, to perform a thorough and independent audit annually. (Civ. Code § 1798.185(a)(14)(A).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The regulations provide flexibility for businesses and do not require businesses to implement certain cybersecurity protections or practices, nor do they impose requirements regarding the means by which businesses implement cybersecurity protections or practices. Rather, the regulations provide performance standards for how to comply with the CCPA cybersecurity audit requirement. The Agency will continue to monitor the marketplace as cybersecurity practices evolve, to determine whether modifications to the regulations are necessary.
CS Audits	1787	Comment expresses compliance burden for businesses, particularly small and mid-sized enterprises (SMEs), and proposes tiered compliance mechanisms and incentives for adopting automation and Cybersecurity-as-a-service (CaaS) solutions.	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations requiring businesses, whose processing of consumers' personal information presents significant risk to consumers' security, to perform a thorough and independent audit annually. (Civ. Code § 1798.185(a)(14)(A).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The Agency has revised the regulations to simplify implementation for businesses, and significantly reduce the costs of the regulations on small businesses. The Agency also revised §

			7121(a) to phase in implementation by annual gross revenue over a three-year period. This will provide small businesses additional time to come into compliance. The regulations provide flexibility for businesses and do not require businesses to implement certain cybersecurity protections or practices, nor do they impose requirements regarding the means by which businesses implement cybersecurity protections or practices. Rather, the regulations provide performance standards for how to comply with the CCPA cybersecurity audit requirement.
CS Audits	1800	Comment is concerned with the DROP tool in which registered data brokers, their vendors, and customers will have access to personal identifiers; and requests that the Agency conduct and publish the mandatory cybersecurity audit required by the State of California as an appendix to the same cybersecurity audit mandated under these draft regulations.	To the extent the comment refers to audits that the Agency would undergo, the comment is not on the proposed action, as the regulations require "businesses" as defined by the CCPA that are subject to the regulations to perform a cybersecurity audit, not the Agency. To the extent the comment refers to the DROP regulations, the comment is not on the proposed action, but the Agency notes comment's suggestion and encourages commenter to participate in the rulemaking process for the DROP regulations.
CS Audits	1807	Comment argues that businesses can reward or penalize conscientious consumers who practice good cybersecurity hygiene, abide by Terms & Conditions, and report concerns that could endanger themselves and others. If businesses would reward these consumers for their diligence, they might attract more satisfied customers, dedicated employees, and impact-investors.	It is unclear what the comment is suggesting the Agency do in the regulations; however, the Agency agrees that businesses can encourage consumers to be diligent about cybersecurity and believes that the cybersecurity audit regulations support businesses' protection of consumers' personal information.
CS Audits	1811	Comment supports the Agency's cybersecurity audit requirements and commends the Agency for its inclusive approach.	The Agency agrees with this comment to the extent it supports the Agency's regulations and notes comment's support.

CS Audits	1816	Comment suggests clarifying that the intent of the audit is to identify non-compliance with the business's documented cybersecurity program.	The Agency agrees with this comment to the extent it supports the benefits of cybersecurity audits. Cybersecurity audits help businesses to identify and address cybersecurity vulnerabilities, motivate businesses' senior leadership to invest in improving the business's cybersecurity, and mitigate the negative impacts of unauthorized access, destruction, use, modification, or disclosure of personal information; and unauthorized activity resulting in the loss of availability of personal information. However, the Agency does not believe that identifying non-compliance is the sole purpose or that the suggested clarification is necessary at this time.
CS Audits	1819	Comment recommends clarifying requirements that apply pre-audit (i.e. preparation) or post-audit (i.e. follow-up activity). This sets clear expectations for both businesses and auditors and promotes order and organization.	The Agency disagrees with this comment. The regulation is reasonably clear based on the plain meaning of the words and specifically identifies the requirements. In addition, the Agency has revised the regulations to provide additional clarity about how businesses and their auditors must complete a cybersecurity audit. The Agency believes that no further clarification is needed at this time.
CS Audits	1903	Comment commends the Agency's effort to address the serious issue of data breaches that have affected billions of records and caused consumer harm. The regulations' requirement that all covered businesses conduct regular cybersecurity assessments is an essential first step in reducing the risk of data compromise. Comment recommends the Agency to expressly encourage covered businesses to seek out cybersecurity services rooted in nationally recognized standards sets, such as NIST 800-53, SOC-2, and ISO 27001. Comment also suggests the Agency to consider implementing a program whereby security	The Agency agrees in part with this comment. The Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example. The regulations implement the requirements of California law, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements. The Agency will continue to monitor the marketplace as cybersecurity and cybersecurity auditing practice evolve, to determine whether modifications to the regulations are necessary, including the comment's suggestion.

		assessment vendors can become certified to offer Agency-compliance services.	
CS Audits	2004	Comment asserts that the cybersecurity provisions overlook practical considerations and outcomes, which at some point start to require the dedication of more resources to conducting audits than to protecting against threats.	The Agency disagrees with this comment and has made efforts to limit the burden of the regulations while implementing the CCPA.
CS Audits	2009, 1298, 1325, 1524	Comment asserts that the cybersecurity audit requirements fail to recognize industry standard risk-based frameworks already in place. For example, the audit requirements disregard widely accepted frameworks such as NIST, which businesses are already used to enhance security. Likewise, comment asserts that under § 7123(b), which mandates justification for 44 separate security controls, businesses would be required to implement security controls that may not be applicable to the company's operations. Comment further indicates that requiring businesses to explain why they are not using a specific technology, such as multi-factor authentication, ignores the fact that companies following recognized cyber security frameworks have determined that certain technologies may not be appropriate based on the risk associated with their processing activities. Comment also warns of the complexities with implementing the audit requirements.	The Agency disagrees with this comment. Nevertheless, the Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example. The CCPA directs the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The regulations are consistent with this direction and do not require businesses to implement certain cybersecurity protections or practices. Rather, they provide clarity about how businesses must perform a thorough and independent cybersecurity audit. After again reviewing the listed components in § 7123(c), the Agency has determined they are consistent with other cybersecurity frameworks and the CCPA's provision that the Agency establish a process to ensure that audits are thorough while providing flexibility to businesses. However, the Agency revised § 7123(c), previously § 7123(b)(2), to further clarify that the audit must assess listed components of a cybersecurity program that the auditor deems applicable to the business's information system. The Agency has 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, to simplify implementation at this time.

ARTICLE 10. RISK ASSESSMENTS

Section of Regulation	Comment Numbers	Summary of Comments 45-Day Comment Period	Agency Response
7150	253, 988, 1928	Comment suggests that the proposed regulations should define processing that presents a "significant risk" to consumers' privacy in line with other global and state privacy laws, such as the Colorado Privacy Act. Comment suggests following other jurisdictions but removing reference to disparate treatment because that is a civil rights' issue and not supported by the CCPA. Businesses should also be allowed flexibility in defining "minimum necessary" personal information due to evolving data processing needs.	The Agency disagrees with this comment. The risk assessment regulations are consistent with other jurisdictions, such as the EU and Colorado, while furthering the intent and purposes of the CCPA. Further, discrimination is a privacy harm, as set forth in § 7152(a)(5), which is consistent with the intent and purposes of the CCPA. The regulations have also been revised to further simplify implementation for businesses at this time and provide clarity on what types of processing requires a risk assessment. The "minimum necessary" personal information language provides guidance to businesses about the relevant standard for processing personal information when identifying categories of personal information in § 7152(a)(2). With respect to evolving data processing needs, the regulations enable businesses to update their risk assessments when there is a material change.
7150	602	Comment argues that the definition of ADMT is overly broad, leading to unnecessary and costly risk assessments for activities that pose little or no privacy risk. Comment believes this exceeds the Agency's authority and suggest narrowing the triggers for risk assessments to focus on high-risk use cases. Comment proposes removing the illustrative example in subsection (c)(6) to avoid the implication that any use of facial recognition to establish identity, whether	The Agency disagrees with this comment. Defining ADMT is within the Agency's delegated authority, as is requiring risk assessments for processing that presents significant risk to consumers' privacy, including for uses of ADMT and facial recognition. (*See* Civ. Code § 1798.185(a)(14)-(15).) The definition of ADMT provides clear guidance about the types of technologies impacted. The Agency has also revised the definition to focus on the level of human involvement. With respect

		it is the sole basis to make significant decisions or not, is ADMT. Comment also opposes requiring risk assessments for AI training and behavioral advertising.	to the training threshold, training the types of technologies identified in the threshold, including facial recognition technology, presents significant risk to consumers' privacy. Training these technologies poses that risk, regardless of whether they are the sole basis to make a decision regarding a consumer. The example regarding facial recognition technology has also been revised for consistency with the training threshold. Further, the profiling for behavioral advertising threshold has been removed to simplify implementation for businesses at this time.
7150	649, 650	Comment states that the regulations impermissibly introduce brand new concepts, in particular the concept of "behavioral advertising." Regulations should focus on activities that involve sensitive data, rather than assuming all advertising is high-risk. The enabling regulatory language, in fact, only references risk assessments for processing sensitive personal information, and it is questionable whether the Agency has authority to require risk assessments for selling, sharing, using ADMT for a significant decisions or extensive profiling, or using personal information to train ADMT. The requirements are unnecessary and lack interoperability.	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purposes of the CCPA. (*See* Civ. Code § 1798.185(a)(14).) Risk assessments must address processing that presents significant risk to consumers' privacy, even if the processing does not include sensitive personal information. Each of the activities listed in § 7150(b) presents significant risk to consumers' privacy. Further, the profiling for behavioral advertising threshold has been removed to simplify implementation for businesses at this time. The risk assessment thresholds are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the intent and purposes of the CCPA and providing clarity and guidance to businesses regarding what is in scope.
7150	651	Comment raises concerns about the impact of the proposed regulations on non-profit versus for-profit institutions, particularly in the education sector. Comment argues that requiring DPIAs for for-profit universities, but exempting non-profits, gives state institutions a competitive advantage.	The Agency disagrees with this comment. The CCPA applies to "businesses" as defined in the CCPA. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The comment also does not explain why businesses conducting risk assessments

			would pose a competitive advantage for state institutions.
7150	696	Comment argues that businesses using vehicle data to influence financial decisions (e.g., insurance pricing, alternative credit scores) should be required to conduct risk assessments.	The Agency agrees in part with this comment, to the extent it supports the regulations. Using ADMT to make a significant decision requires a risk assessment. If an ADMT is processing personal information about a consumer's vehicle usage to make a significant decision about them, the business would be required to conduct a risk assessment pursuant to § 7150(b)(3).
7150	796	Comment is concerned these provisions are overly burdensome. Content requirements such as "specifically identifying business purposes for consumer process; specifically identifying benefits to the business; number of consumers whose personal information is processed; and contributors to the risk assessment" is essentially asking businesses to reveal company and client confidential information and/or business-trade secrets. There is also significant risk of downstream impact on smaller businesses through partnerships with larger companies that could be subject to compliance. There are no exemptions for non-ADMT developers or service providers.	The Agency disagrees with this comment. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. In addition, the Agency has revised Article 10 overall to simplify implementation for businesses at this time, including clarifying what must be included in a risk assessment report and how to identify purposes and benefits with specificity. The requirements regarding identifying the purpose and relevant benefits are necessary to appropriately conduct a risk assessment. With respect to number of consumers whose personal information is processed and contributors, this information is necessary to identify risk and to ensure the business has identified who contributed information to the risk assessment. The contributors to the risk assessment are necessary to ensure accuracy and accountability in the risk assessment process. When providing the required information, the CCPA does not require a business to divulge trade secrets. No exemption is necessary, because the CCPA's risk assessment requirements apply to "businesses" as defined by the CCPA. §§ 7050 and 7153 also help ensure smaller businesses can comply, because service providers, contractors, and businesses that train certain ADMT must provide all

			facts necessary to the business to conduct the risk assessment.
7150	869	Comment asserts that the rules in § 7150 for when a business shall conduct a risk assessment should reflect actual risks and avoid broad, sweeping language.	The Agency disagrees with this comment. The risk assessment regulations are not overly broad, but rather address processing activities that present significant risk to consumers' privacy. They are consistent with other jurisdictions, such as the EU and Colorado, while furthering the intent and purposes of the CCPA.
7150	1010	Comment argues that behavioral advertising should not be categorized as "extensive profiling" because ads do not make autonomous decisions; rather, they provide opportunities for businesses to reach potential customers. It is also inconsistent with the statute and will have significant downstream consequences.	The Agency disagrees with this comment. However, the Agency has removed profiling for behavioral advertising from the risk assessment thresholds to further simplify implementation for businesses at this time.
7150(b)	1708	Comment recommends revising § 7150(b) as follows: "Each of the following processing activities presents significant risk to consumers' privacy: (3) Using automated decisionmaking technology as the sole basis to make significant decision concerning a consumer."	The Agency disagrees with this comment. The ADMT definition is clear about what technologies were in scope and was not overly expansive. Exercising its discretion, the Agency revised the definition of ADMT to focus on the level of human involvement, which furthers both consumer privacy and simplifies implementation for businesses at this time. Comment's recommendation is also less clear and less effective than the regulation at protecting consumer privacy.
7150(b)	505, 531, 1995	Comment argues that requiring risk assessments for internal AI model development is unnecessary and hinders innovation. Training ADMT or AI and behavioral advertising should not trigger a risk assessment.	The Agency disagrees with this comment. The CCPA requires risk assessments for processing that presents significant risk to consumers' privacy. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The regulatory requirements are necessary and do not hinder innovation. By contrast, they balance providing privacy protections for consumers with flexibility for businesses

			to come into compliance. Additionally, the regulation has been revised to further simplify implementation for businesses at this time, including using an intent-based standard for training and removing profiling for behavioral advertising.
7150(b)	1055	Comment asserts that not all sharing of personal information should necessitate a risk assessment. For instance, most organizations share minimal personal information with third parties for advertising purposes. Requiring extensive risk assessments for such de minimis data-sharing activities diverts focus from more critical and high-risk data-sharing practices. Comment also objects to the inclusion of the behavioral advertising threshold. Further, comment states that many processing activities, particularly those with minimal data use, have neutral or even positive effects on consumers. Applying the balancing test as proposed may lead to inconsistent outcomes across organizations, undermining the clarity and predictability essential for compliance.	The Agency disagrees with this comment. Sharing of personal information presents significant risk to consumers' privacy. In addition, comment's recommendation is less effective than the regulation. Businesses would have no way of determining what is and is not de minimis data sharing, nor does the comment propose what this would mean. The Agency does not believe that the behavioral advertising threshold is overly broad but has removed it to further simplify implementation for businesses at this time. Further, the regulations provide clear guidance on how to conduct a risk assessment that can be adapted to variety of industries and use cases, and do not lead to inconsistent outcomes.
7150(b)	1912, 1914	Comment states that the criteria for risk assessments is so broad that it will hurt the cause of privacy. It scopes in any business using software. This will burden businesses and overwhelm the CPPA with paperwork, diminishing its focus on enforcement. § 1798.185(a)(15) mandates risk assessments only for activities posing "significant risks to privacy or security," yet these regulations use ADMT as a trigger. But ADMT does not inherently impact privacy and was specifically omitted from this part of the statute precisely because one of the main organizing principles in the drafting, was to be technology-	The Agency disagrees with this comment. The risk assessment thresholds each address processing that presents significant risk to consumers' privacy. The Agency also provides ample evidence of the privacy risks associated with businesses' use of ADMT, including a lack of transparency for consumers to know when a business is using ADMT with respect to them, a lack of consumer control over how their personal information is processed using ADMT, and unlawful discrimination. Further, the Agency has revised the regulations to further simplify implementation for businesses at this time.

		agnostic. The statute emphasizes the nature of the activity, not the technology involved.	
7150(b)	1438	Comment suggests clarifying that the requirement to conduct a risk assessment when a business uses ADMT to make a significant decision concerning a consumer refers to the entity that uses the automated decisionmaking system. Comment also suggests deleting the "extensive profiling" provisions in § 7150(b)(3)(B).	The Agency disagrees with this comment. The CCPA requires businesses to conduct risk assessments for processing activities that present significant risk to consumers' privacy. The Agency determined that a business's use of ADMT to make a significant decision concerning a consumer presents significant risk to consumers' privacy. The regulations are already clear that a business using ADMT to make a significant decision concerning a consumer must conduct a risk assessment. The Agency deleted the extensive profiling threshold and revised the regulations to focus on the use of ADMT without any human involvement for significant decisions.
7150(b)(2)	990	Comment recommends aligning § 7150(b)(2) with existing sensitive personal information (SPI) exceptions in § 7014(g) to ensure consistency in regulatory requirements.	The Agency disagrees with this comment. The exemptions in § 7014 address when certain disclosures need to be provided to consumers. Risk assessments are about identifying risks to consumers' privacy. For example, even if a business is not using a social security number to infer characteristics about a consumer, processing this information can still pose risk to consumers' privacy, such as the risk of unauthorized access if the information is not stored securely.
7150(b)(2)	1434	Comment suggests revising this threshold to reflect the processing of SPI of 1 million or more consumers or households in the preceding calendar year.	The Agency disagrees with this comment. Comment's proposed volume threshold is less effective than the regulation because it would exclude processing activities that pose significant risk to consumers' privacy. It also is not consistent with other jurisdictions' approaches, which do not limit risk assessments using the volume-based threshold proposed.

7150(b)(2)(A)	989	Comment argues that § 7150(b)(2)(A) should broaden exemptions for routine personnel activities involving sensitive information. They contend that many such activities were not included in the regulation but align with the intent to reduce assessment burdens. Examples include tracking employees' dietary restrictions and mobility needs.	The Agency agrees in part with this comment. The Agency has revised the exception in § 7150(b)(2)(A) to include providing reasonable accommodations required by law. However, the comment does not define "routine" personnel activities; thus, it does not provide sufficient clarity to businesses about what activities are in scope of the exception. By contrast, the activities listed in § 7152(b)(2)(A) provide clarity about the types of personnel activities that are exempted from § 7152(b)(2).
7150(b)(3)	404	Comment argues that the proposed regulations define "significant risk" inconsistently across different contexts (risk assessments vs. cybersecurity audits). § 7150(b)(3) is too broad — it includes any "significant decision" involving ADMT. The definition should align with GDPR, limiting "significant decisions" to those with "legal or similarly significant effects."	The Agency disagrees with this comment. Cybersecurity audits address processing that presents significant risk to consumers' security. Risk assessments address processing that presents significant risk to consumers' privacy. In addition, the scope and nature of a cybersecurity audit are different from those of a risk assessment, which necessitates different regulations to provide clarity to businesses about how to conduct each one. The definition of "significant decision" is consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. Additionally, the definition of significant decision has been revised to further simplify implementation for businesses at this time.
7150(b)(3)	744, 745	§ 7150(b)(3) is overbroad and inconsistent with the statute, incorporating into the scope of the requirement any "significant decision" using ADMT. Comment suggests that this provision should be revised to include a definition of "significant decision" that mirrors the GDPR concept of "legal or similarly significant effects."	The Agency disagrees with this comment. Under the CCPA, risk assessments are required for processing that presents significant risk to consumers' privacy. This includes using ADMT to make a significant decision about a consumer. The regulation balances providing privacy protections for consumers with flexibility for businesses to come into compliance. In addition, the

			definition of "significant decision" is consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. Additionally, the definition of significant decision has been revised to further simplify implementation for businesses at this time.
7150(b)(3)	1488	Comment suggests striking inclusion of "using automated decisionmaking technology for a significant decision concerning a consumer or for extensive profiling" in § 7150(b)(3). Comment also suggests striking additional references to ADMT throughout the Article. The CCPA provides clear direction to the Agency regarding its regulatory authority regarding ADMT; the statute specifies the issuance of regulations "governing access and opt-out rights with respect to businesses' use of automated decisionmaking technology." There is no mention of including ADMT in risk assessments.	The Agency disagrees with this comment. The comment misreads the CCPA's delegation of authority to the Agency. For risk assessments, the Agency must issue regulations requiring risk assessments for processing that presents significant risk to consumers' privacy. (Civ. Code § 1798.185(a)(14).) This includes the use of ADMT for a significant decision and extensive profiling. Separate from risk assessments, the Agency also must issue regulations regarding access and opt-out rights for businesses' use of ADMT. (Civ. Code § 1798.185(a)(15).) These regulations are not mutually exclusive. Rather, a business using ADMT for a significant decision must conduct a risk assessment and comply with the access and opt-out requirements for that ADMT.
7150(b)(3)	1598, 1600	Comment states that any classification of "significant risk" processing in § 7150(b) should be rebuttable through a business's own contextual risk assessment. They warn that rigid, categorical lists of high-risk activities could result in overregulation of and under-regulation. A rebuttable presumption within a risk-based approach supplemented with guidance makes risk assessments practicable and scalable, enabling case-by-case risk and mitigation determinations. This approach would allow more accurate classification and mitigation of risks, avoid unnecessary regulation	The Agency disagrees with this comment. Comment's proposed rebuttable recommendation is less effective than the regulation at protecting consumer privacy. It also is less clear than the regulation because it does not clearly indicate how a business would rebut the classification of a processing activity in § 7150(b) as a significant risk. The regulations also provide sufficient guidance to businesses regarding the thresholds and how to conduct a risk assessment and are both practicable and scalable.

		of low-risk activities, and ensure that the Agency focuses on truly high-risk processing.	
7150(b)(3)	1917	The regulations should remove "essential goods and services." If it is not removed, then clarify what qualifies as "essential" to avoid unnecessary assessments.	The Agency agrees in part with this comment, to the extent it requests removal of the term. The Agency has removed "essential goods or services" in the definition of significant decision to simplify implementation for businesses at this time. The Agency disagrees in part with this comment, to the extent that it suggested that the term would have been unclear.
7150(b)(3)(A)	273, 1544, 1622	Comment argues that the regulations unnecessarily require risk assessments for all profiling activities, even when they do not result in legally significant decisions, such as financial, housing, or employment decisions. This broad approach creates excessive burdens for businesses, particularly since some impacts on consumers are speculative. Terms like "access to" services and "compensation" are too vague and should be clarified or limited. Risk assessments should only apply to profiling tied to significant decisions or actual employment opportunities. Comment also states it is difficult to provide an opt-out for this profiling, and that the regulation departs from other state laws and should not include terms such as "access to" and "independent contracting opportunities or compensation."	The Agency disagrees with this comment. Risk assessments are required for processing activities that present significant risk to consumers' privacy, regardless of whether they render a significant decision about a consumer. This includes certain automated processing in the workplace or in educational settings, or in sensitive locations. Contrary to comment's point, this is not a requirement for all profiling, but rather certain automated processing that can cause several negative impacts to consumers' privacy, such as less consumer control over personal information, insufficient transparency, excessive surveillance, and unlawful discrimination. With respect to comment's point on burdens, the regulations balance providing privacy protections to consumers with flexibility for businesses to come into compliance. They also have been revised to further simplify implementation for businesses at this time. In addition, the harms to consumers from this processing are not speculative, but rather pose several risks to consumers, such as lack of transparency and meaningful control over their personal information. Additionally, "access to" has been removed to simplify implementation at this time. The terms "independent contracting opportunities or compensation" and

			"compensation" are reasonably clear and the Agency does not believe they require additional clarification, or warrant removal because independent contracting decisions and compensation decisions are significant to consumers. With respect to the opt-out requirements in Article 11, this has been limited to use of ADMT for significant decisions. Further, the regulations are consistent with other state laws while furthering the intent and purposes of the CCPA.
7150(b)(3)(A)	327, 328, 329	Comment raises concerns about the language in § 7150, particularly subsection (b)(3)(A), which defines "significant decisions." Comment argues that the proposed regulations may inadvertently exempt insurers and financial services companies from risk assessment requirements when using ADMT. Comment argues that the GLBA, while providing a baseline for consumer data protection, does not adequately regulate large-scale automated decision-making systems. Since the GLBA predates modern ADMT, insurers and financial service providers could interpret the proposed regulations as permitting them to use consumer data in ADMT systems without undergoing the necessary risk assessments. This could lead to unregulated, high-stakes decisions about financial services and insurance. Comment urges the Agency to explicitly state in § 7150 that all significant decisions involving personal data — even if the data is subject to GLBA protections — must undergo risk assessments. Comment argues that financial and insurance companies should not be able to use ADMT without regulatory oversight.	The Agency disagrees with this comment. The CCPA provides exemptions for certain information subject to GLBA and FCRA. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The regulations apply only to personal information subject to the CCPA. Financial or lending services that are not subject to a CCPA exemption are subject to this risk assessment threshold, if they are using ADMT for a significant decision. Nevertheless, the Agency has removed the reference to insurance to simplify implementation at this time.
7150(b)(3)(A)	1435	Comment suggests revising to include "unless exempt by statute or as otherwise set forth in these rules,"	The Agency disagrees with this comment. The regulations do not amend the CCPA, so language

		deleting references to Civil Code §§ 1798.145 and 1798.146, deleting "access to, or the provision or," and adding "in emergency situations" when referring to fuel.	regarding the statutory exemptions is not necessary. The Agency has removed references to Civil Code §§ 1798.145 and 1798.146 accordingly. In addition, the Agency has removed "access to" and "essential goods or services" in the definition of significant decision to simplify implementation for businesses at this time. Further, a business that uses ADMT to provide consumers with a type of significant decision can still pose significant risk to consumers' privacy, so the term "provision" has been retained in the definition of significant decision.
7150(b)(3)(A)(i)–(ii)]	1436, 1437	Comment suggests revising the thresholds regarding "education or enrollment opportunity" and "employment or independent contracting opportunity or compensation" to say "means" instead of "includes." Comment also suggests deleting subsection (ii)(2) except for the reference to "salary."	The Agency agrees in part with this comment, to the extent it suggests using "means," and the Agency revised the regulations accordingly. The Agency disagrees with the comment's suggestion to delete portions of subsection (ii)(2). Allocation or assignment of work and compensation are significant decisions for consumers. However, the Agency narrowed allocation or assignment of work to employees to further simplify implementation for businesses at this time.
7150(b)(3)(B)	169	Delete reference to "extensive profiling" in § 7150(b)(3) and the entirety of § 7150(b)(3)(B). If not, comment suggests alternative language that references the CCPA statutory exceptions.	The Agency agrees in part with this comment, to the extent it requests removal of the term "extensive profiling." The term "extensive profiling" has been deleted, but businesses must conduct risk assessments for certain automated processing in the workplace and in sensitive locations that present significant risk to consumers' privacy, as set forth in §§ 7150(b)(4)-(5). The Agency otherwise disagrees with this comment. The revised regulations ensure that businesses conduct a risk assessment for certain automated processing that presents significant risk to consumers' privacy. In addition, the proposed alternative is unnecessary, because the regulations do not amend the CCPA's

			exemptions, which apply to the regulations. The Agency has revised the risk assessment regulations to remove the profiling for behavioral advertising threshold, to further simplify implementation for businesses at this time.
7150(b)(3)(B)	274, 1545, 1623	Comment argues that risk assessments should only be required when legally significant decisions are made using a consumer's profile. The current provisions in § 7150(b)(3)(B) are duplicative and overly broad. The framework for "extensive profiling" does not offer additional privacy protections and duplicates requirements under § 7150(b)(3)(A) for significant work and education decisions. Moreover, the provision likely exceeds the scope of the CCPA.	The Agency disagrees with this comment. The use of ADMT for significant decisions is not the only processing activity that presents significant risk to consumers' privacy. Other automated processing in the workplace is included in the risk assessment framework because it poses significant risk to consumers' privacy, regardless of whether the processing is for significant decisions or other uses by the business. This automated processing that can cause several negative impacts to consumers' privacy, such as less consumer control over personal information, insufficient transparency, excessive surveillance, and unlawful discrimination. Further, this threshold is within scope of the CCPA, as set forth in the plain text of the delegation to the Agency in Civil Code § 1798.185(a)(14), which requires the Agency to issue regulations for risk assessments for processing that presents significant risk to consumers' privacy. This delegation is not limited to processing for significant decisions, and comment's recommendation would be inconsistent with the statutory delegation. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
7150(b)(3)(B)	1439	Comment suggests including that a business required to complete a risk assessment under (a)(3) refers to the entity that uses the ADMT.	The Agency disagrees with this comment. The regulation is clear. A business that is using ADMT to make a significant decision concerning a consumer must conduct a risk assessment. § 7050 also makes clear that service providers and contractors must

			cooperate with the business that is conducting the risk assessment.
7150(b)(3)(B)(i)-(ii)	1877	Comment argues that these two sections are excessive and unnecessary. They include low-risk technologies like CCTV. These two sections should be removed.	The Agency disagrees with this comment. Risk assessments are required for processing activities that present significant risk to consumers' privacy, regardless of whether they render a significant decision about a consumer. This includes certain automated processing in the workplace or in educational settings, or in sensitive locations. Contrary to comment's point, this is not a requirement for all profiling, but rather certain automated processing that can present significant risk to consumers' privacy, such as less consumer control over personal information, insufficient transparency, excessive surveillance, and unlawful discrimination.
7150(b)(3)(B)(iii)	1599	Comment expresses concern over the inclusion of all behavioral advertising-related profiling as "significant risk" under § 7150(b)(3)(B)(iii). They argue that many such profiling activities pose minimal risk and should not be treated as inherently high-risk. Comment believes businesses should be able to complete risk assessments to rebut the presumption that this kind of processing involves significant risk, and risk assessment submissions to the Agency should not be required when these determinations are made. However, businesses should maintain records of these risk assessments and submit them to the Agency or Attorney General when requested to do so.	The Agency disagrees with this comment. The goal of risk assessments and their submission to the Agency are explicitly outlined in the CCPA. Submission only of certain risk assessments is not consistent with the CCPA. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Further, profiling for behavioral advertising does not pose only minimal risk to consumers' privacy. However, the Agency has removed this threshold from the risk assessment regulations to further simplify implementation for businesses at this time.
7150(b)(3)(B)(iii)	1881	Comment believes that this subsection is excessive and circular based on the definition of "behavioral advertising." Comment claims that § 7150(b)(3)(B)(iii) would require a risk assessment for almost any personalized advertising, regardless of the topic or	The Agency disagrees with this comment. The definition of behavioral advertising is clear and is neither excessive nor circular. Nevertheless, the Agency has removed the definition and corresponding risk

		subject matter, which is excessive. This subsection should be removed.	assessment threshold from the regulations to further simplify implementation for businesses at this time.
7150(b)(6) [previously 7150(b)(4)]	170	Comment suggests deleting this subsection in its entirety, or revising it as follows: "Processing the personal information of consumers to train automated decisionmaking technology or artificial intelligence that is designed to be used for any of the following (but excluding the processing of personal information that is subject to, or the training of automated decisionmaking that is designed to be used with personal information that is subject to, one or more exceptions set forth in Civil Code sections 1798.145, subdivisions (c)-(g), or 1798.146, subdivisions (a)(1), (4), and (5))."	The Agency disagrees with this comment. The regulations ensure that businesses conduct a risk assessment for certain training uses of personal information that present significant risk to consumers' privacy. In addition, the proposed alternative is unnecessary, because the regulations do not amend the CCPA's exemptions. Further, the regulation has been revised to use an intent-based standard.
7150(b)(6) [previously 7150(b)(4)]	1719	Comment suggests removing "or profiling" in the section.	The Agency disagrees with this comment. The training uses of personal information in this threshold, including for certain profiling, present significant risk to consumers' privacy. Further, the Agency has revised the regulation, including using an intent-based standard, to further simplify implementation for businesses at this time.
7150(c)	991	Comment appreciates that inclusion of illustrative examples and suggests adding an additional example involving the internet of things.	The Agency agrees with this comment and notes comment's support for the inclusion of examples. The Agency does not believe it is necessary to include an example involving the internet of things at this time.
7150(c)(1) [previously 7150(c)(2)]	1440	Comment suggests revising the example to state that the use of the ADMT would be dispositive as to whether the employee advances further in the hiring process and to delete references to physical or biological identification and profiling.	The Agency disagrees with the comment. The suggested language is less clear than the language in the regulation. The Agency has also revised the language in the example to reflect the scope of the revised ADMT threshold in § 7150(b)(3), and deleted reference to physical or biological identification and profiling because it is duplicative.

DRAFT

7150(c)(1) [previously 7150(c)(2)]	1720	Comment suggests removing "or profiling" in the section.	The Agency disagrees with this comment. However, the Agency has revised the example to align with the revised definition of ADMT, which focuses on human involvement. This definition still includes profiling when used without human involvement.
7150(c)(5)	924	Comment claims that § 7150(c)(5) improperly includes Media Access Control ("MAC") address processing as an example requiring a risk assessment, even though MAC addresses do not identify individuals. This example should be removed to align with the "significant risk" standard.	The Agency disagrees with this comment. MAC addresses can be used to identify individuals. However, the Agency has removed the example, because the public profiling threshold has been removed.
7151	1073	Comment calls for clarifying the role of community stakeholders in risk assessments to ensure that impacted groups have a voice in evaluating the risks associated with automated decision-making.	The Agency disagrees with this comment, to the extent that it argues that the regulations are not clear. § 7151 is clear that businesses may consult with external parties as part of the risk assessment process. This provides clarity and guidance to businesses about what stakeholders they may consider including in the risk assessment process while providing flexibility to businesses to identify who should be included.
7151(a)	107, 1082	Comment recommends incorporating workers and unions into risk assessment processes for ADMT and data processing, as workers have firsthand knowledge that can help identify risks and improve implementation. Comment suggests clarifying their roles, such as adding language to § 7151(a) to require "meaningful consultation" with employees, contractors, and unions in risk assessments.	The Agency disagrees with this comment. Businesses are not prohibited from with consulting with employees, contractors, or unions. The current language provides clarity and guidance to businesses about what stakeholders they may consider including in the risk assessment process while providing flexibility to businesses to identify who should be included. Comment's recommendation is not necessary at this time.
7151(a)	1441	Comment suggests deleting reference to fraud prevention.	The Agency disagrees with this comment. A business may need to include individuals on a fraud prevention team as part of conducting a risk assessment for a processing activity. However, the Agency has revised

			the example to address an individual who determines the method by which the business plans to collect personal information, to provide further clarity about how an individual would have necessary information for conducting the risk assessment.
7151(b)	450	Comment recommends that the Agency require independent evaluations by socio-technical experts to identify and mitigate potential biases in ADMT systems, specifically in § 7151(b). Comment advocates for the inclusion of non-affiliated third-party evaluators with expertise in bias, AI ethics, technical auditing, and societal factors to improve risk assessments and ensure impartiality.	The Agency disagrees with this comment. § 7151(b) is clear that businesses may consult with external parties as part of the risk assessment process. This provides clarity and guidance to businesses about what stakeholders they may consider including in the risk assessment process while providing flexibility to businesses to identify who should be included. The Agency does not believe mandatory independent evaluations are necessary at this time.
7151(b)	106	Comment calls for reinstating a provision that requires businesses to provide a plain-language explanation if they do not consult external parties and to outline additional safeguards implemented as a result.	The Agency disagrees with this comment. The Agency has chosen not to require this explanation to simplify implementation for businesses at this time.
7151(c)	1254	Comment claims that § 7151(c) would apply disclosure and opt-out rights even when businesses use consumer data for internal AI training, not just direct consumer decision-making. Comment argues that internal AI training does not translate to direct harm.	Comment has cited § 7151(c), which is not a provision in the regulations. However, with respect to harm, the Agency disagrees with the comment that consumers' privacy is not at risk due to training uses of ADMT. Nonetheless, the Agency has removed training uses of ADMT from the scope of Article 11's notice and opt-out requirements to further simplify implementation for businesses at this time.
7152	102, 1081	Comment agrees that the proposed regulations provide a necessary framework to ensure that businesses assess the risks of ADMTs to both consumers and workers. While the current draft includes key protections, additional enhancements are needed to improve transparency and accountability	The Agency agrees in part with this comment and notes comment's support. The proposed regulations provide transparency and accountability and ensure privacy risks and safeguards are identified. They have been revised to provide additional clarity and to simplify implementation for businesses at this time. The Agency

		and to ensure the potential harms of ADMTs are evaluated and mitigated.	does not believe that additional modifications are necessary.
7152	201	Comment suggests the following revisions to decrease the prescriptive nature of the regulations. First, for subsection (a)(1): use only "The business must specifically identify its purpose for processing consumers' personal information." Comment suggests removing the second sentence in (a)(1) regarding not identifying a purpose in generic terms. Second, for subsection (a)(2), comment suggests adding "of the following, as applicable" to this sentence as follows: "The business must identify the categories of personal information to be processed and whether they include sensitive personal information. This must include discussion of the following, as applicable[.]" Third, for subsection (a)(6), comment suggests adding the word "collectively" to this sentence as follows: "The business must identify the safeguards that it plans to implement to address the negative impacts identified in subsection (a)(5). The business must specifically identify how these safeguards collectively address the negative impacts identified in subsection (a)(5), including to what extent they eliminate or reduce the negative impacts; and identify any safeguards the business will implement to maintain knowledge of emergent risks and countermeasures."	The Agency disagrees with this comment. The recommendation makes § 7152(a)(1) less clear about how a business must identify a purpose for processing consumers' personal information. The Agency also has revised § 7152(a)(1) to provide additional guidance about how to identify a purpose for the risk assessment that is not in generic terms. With respect to § 7152(a)(2), the Agency has revised the regulation to further simplify implementation for businesses at this time, including requirements regarding quality of personal information. The regulation also provides more clarity than the recommended language about the categories of personal information and sensitive personal information that must be identified. Similarly, with respect to § 7152(a)(6), the Agency has revised the regulation to further simplify implementation for businesses at this time, so that businesses identify and document any safeguards it plans to implement for the processing activity. Comment's recommendation is not necessary, because that requirement has been removed.
7152	255, 256, 603, 870, 1052, 1725	Comment suggests that the proposed regulations should revise the requirements for the content to be included in risk assessments. Comment states that they are extensive and go beyond existing requirements, including not identifying a purpose in generic terms, identifying certain operational elements, identifying profit and hypothetical harms,	The Agency disagrees with this comment. The requirements provide clarity to businesses as to what information is necessary to adequately identify the benefits and potential risks of a given processing activity. The requirements are consistent with the CCPA and with approaches taken in other jurisdictions, such as the EU and Colorado, and are not overly technical or

		and identifying whether the business will initiate the processing. In addition, the Agency should revise the content to be included in risk assessments by modifying § 7152(a)(6)(B)(iii)(1) to state: "Where a business obtains the automated decisionmaking technology from another person, the business must identify how it evaluated the technology." Comment also suggests that the Agency should harmonize the content of risk assessments in § 7152 with requirements under other state and global privacy laws. Comment argues that the regulations require businesses to include unnecessary technical and business details in risk assessments, such as intended output, logic, and expected profits. Comment claims these requirements exceed other standards like GDPR and shift the focus from identifying risks to excessive documentation. Comment also proposes adjustments to the rigid timing requirements contemplated in the regulations to provide flexibility for the varied processing activities of businesses, without adverse impact on consumers. Further, comment recommends replacing or significantly editing § 7152 to better align with statutory intent and international norms. Comment raises concerns that § 7153's disclosure requirements would prioritize complicated pro forma exercises over careful evaluation and remediation of risks and run contrary to CCPA instructions.	burdensome. Identifying the purpose in non-generic terms and operational elements are necessary for a business to identify the relevant risks of that processing activity. Similarly, the negative impacts are provided as guidance so businesses can meaningfully identify risks to consumers' privacy. Additionally, identifying whether the business will initiate the processing activity after identifying the risks is the final step in the risk assessment process, which is necessary to meet the goal of a risk assessment. (*See* Civ. Code § 1798.185.) The Agency has also revised § 7152(a)(6)(B)(iii)(1) to further simplify implementation for businesses at this time, so that a business can consider as a safeguard whether to implement policies, procedures, and training to ensure that the ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics. As part of identifying relevant safeguards, a business may identify how it evaluated the ADMT. With respect to identifying expected profit, the Agency has removed this language. With respect to § 7153, these disclosure requirements ensure that businesses using ADMT for a significant decision have necessary facts to conduct the risk assessment, which assists them in identifying relevant risks to consumers' privacy. Further, the timing requirements are necessary to ensure accuracy and account for material changes in processing activities.
7152	166	Comment suggests that the requirements for risk assessments in § 7152(a) should be adjusted to be less prescriptive, as comparable regimes require a weighing of benefits and risks (as mitigated by safeguards) without imposing requirements to record details that may or may not be relevant to a particular data processing activity. § 7152 is unduly burdensome,	The Agency disagrees with this comment. § 7152(a) provides clear requirements about what information is necessary to conduct a risk assessment and does not require recording of irrelevant or excessively specific details. In addition, these regulations have been revised to further simplify implementation for businesses at this time and provide additional clarity regarding identifying

		lack clear benefits to consumers, and is out of alignment with other states. Comment recommends harmonizing with other U.S. jurisdictions and allowing businesses to be deemed in compliance for reasonably similar risk assessments conducted for other privacy laws. Comment also argues that §§ 7152(a)(5) and 7152(a)(6) require excessive specificity in identifying privacy risks and mitigations without clear benefits to cybersecurity. These provisions conflate privacy and security and could violate First Amendment rights by compelling businesses to disclose risk assessments.	relevant benefits, risks, and safeguards. Together, these requirements ensure businesses conduct meaningful risk assessments, and benefit consumers' privacy by ensuring that consumers are not subject to unnecessary and unmitigated risk to their privacy. These regulations are also consistent with the approaches taken in other jurisdictions, such as those in the EU and in Colorado, while furthering the intent and purposes of the CCPA and providing clarity to businesses regarding their obligations. Further, the Agency does not believe these requirements violate the First Amendment.
7152	1225	Comment states that credit unions already conduct risk assessments under NCUA Part 748, which includes broader security protections. The NCUA standard is stricter because it applies to any reasonably foreseeable threat, whereas the CPPA rule applies only to "significant risk" activities. Comment also raises concerns about the information required for a risk assessment.	The Agency disagrees with this comment, to the extent it argues that the risk assessment requirements are not practical for businesses to comply with. Businesses, such as credit unions, that conduct risk assessments for other laws may leverage their existing compliance processes to meet the requirements in § 7152. (*See* § 7156(b).) § 7152(a) provides clear requirements about what information is necessary to conduct a risk assessment, and does not require recording of irrelevant details. In addition, these regulations have been revised to further simplify implementation for businesses at this time. This approach is also consistent with other jurisdictions, such as the EU and Colorado.
7152	1252	Comment asserts that under § 7152, businesses would be forced to conduct in-depth AI risk assessments of their ADMT systems. Rather than simply informing consumers about automated decision-making, this transforms a privacy law into an AI governance framework and goes far beyond the original legislative text.	The Agency disagrees with this comment. The CCPA requires risk assessments for processing that presents significant risk to consumers' privacy. The use of ADMT to make significant decisions about a consumer presents significant risk to consumers' privacy, and thus requires a risk assessment. With respect to the comment's concerns about the information required for the risk assessment, § 7152(a) provides clear

			requirements about what information is necessary to conduct a risk assessment and does not require recording of irrelevant details.
7152	200	Comment suggests revision as follows: "The business must conduct a risk assessment to determine whether the risks to consumers' privacy from the processing of personal information outweigh the benefits to the consumer, the business, other stakeholders, and the public from that same processing. The business must conduct and document the risk assessment as in accordance with the requirements set forth below, in each case where relevant to the identified significant risk to consumers' privacy and security[.]"	The Agency disagrees with this comment. § 7152 is clear regarding how a business must conduct a risk assessment. The recommendation is not more effective than the regulation at protecting consumer privacy or providing clarity to businesses regarding when a risk assessment is required. The Agency has also revised § 7152 to further simplify implementation for businesses at this time.
7152	697	Comment suggests that the purpose of processing consumers' personal information be explicitly stated and not be described in generic terms such as "safety purposes." The comment also suggests adding "device and data disposal" to the list of safeguards businesses may consider in section (6)(A)(i).	The Agency disagrees with this comment. The regulations are reasonably clear, with examples already provided as guidance. Additional examples are not necessary at this time.
7152	992	Comment recommends modifying § 7152(a) to ensure that risk assessments consider business size and data processing complexity, similar to Colorado and EU regulations. They argue this aligns with statutory language.	The Agency disagrees with this comment. The required elements in § 7152 are relevant for all businesses conducting a risk assessment. To the extent a business seeks to add more information in a risk assessment to address size or complexity, it may do so. With respect to Colorado and the EU, the risk assessment regulations harmonize with their requirements where possible while furthering the purposes of the CCPA and providing clarity and guidance to businesses regarding their obligations.
7152	1196	Comment believes that the draft regulations require extensive risk assessments but fail to provide substantial evidence demonstrating their necessity	The Agency disagrees with this comment. The CCPA requires risk assessments for processing that presents significant risk to consumers' privacy. Each of the

		for consumer privacy. Many required assessment components, such as evaluating the "logic" of algorithms and data reliability, have no direct link to privacy concerns.	processing activities identified in § 7150(b) present significant risk to consumers' privacy and therefore requires a risk assessment. In addition, each of the requirements in § 7152 is necessary to conduct a risk assessment. For example, the identification of the logic of an ADMT used to make significant decisions is necessary to identify potential privacy risks to consumers, such as discrimination. Nevertheless, the regulations have also been revised to further simplify implementation for businesses at this time.
7152	1597	Comment recommends that all processing activities, even presumptively low-risk, should undergo basic risk assessments. These can help identify activities that may trigger more robust assessments under § 7152 of the regulations, especially when guided by rebuttable regulatory classifications.	The Agency disagrees with this comment. The CCPA requires risk assessments for processing that presents significant risk to consumers' privacy. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
7152	1989	The Agency should require algorithmic risk assessments. Businesses should conduct regular risk assessments to evaluate whether their data collection practices adhere to the principles of necessity and proportionality. These assessments will help businesses comply with CCPA provisions like § 7002, which limit data collection to what is necessary, and § 7027, which empowers consumers to restrict the use of sensitive personal information.	The Agency disagrees with this comment. Risk assessments are required for processing that presents significant risk to consumers' privacy. Certain automated processing presents significant risk to consumers' privacy, as set forth in § 7150(b). The risk assessments requirements in § 7152 ensure that businesses have the necessary information to identify relevant risks and benefits. The Agency does not believe that additional requirements are necessary at this time.
7152(a)	1442	Comment suggests revising subsection to reflect that a business conducts risk assessment to "informs its processing activities, including" whether the risks to consumers' privacy from the processing outweighs the benefits.	The Agency disagrees with this comment. The CCPA states the goal of a risk assessment, which is reflected in § 7152(a). The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.

7152(a)(1)	1443	Comment suggests revising subsection to use "may" instead of "must," and removing prohibition against stating the purpose for processing in generic terms.	The Agency disagrees with this comment. Each of the requirements are necessary to ensure that risk assessments are meaningfully conducted and not a paperwork exercise. The suggestion to make these requirements optional undermines the effectiveness of the regulation in protecting consumer privacy.
7152(a)(1)	105, 970	Comment calls for businesses to explicitly state how ADMT processing achieves their purpose and whether that purpose aligns with the original intent of data collection. Comment also asserts that the requirement for businesses to disclose their purpose for processing data is too vague, allowing for meaningless justifications like "security reasons." The December 2023 language should be restored to require detailed explanations.	The Agency disagrees with this comment. § 7152(a)(1) already provides clear guidance for businesses about how to identify the purpose of a processing activity so they can conduct a risk assessment for that activity. To comply with § 7152(a)(3), businesses must identify the planned method for processing personal information, the method of interacting with the consumer, relevant disclosures made to the consumer, the logic of the ADMT, and how the ADMT output will be used to make a significant decision. These operational elements enable businesses to identify whether the ADMT achieves the purpose identified in § 7152(a)(1) and whether the purpose aligns with the original purpose of collecting a consumer's personal information.
7152(a)(1)	993	To avoid vague justifications for data processing, comment proposes revising § 7152(a)(1) to require more specificity in purpose statements.	The Agency agrees in part with this comment. The Agency has revised § 7152(a)(1) to provide additional clarity about how to identify a purpose for the risk assessment that is not in generic terms. The Agency did not use the comment's proposed language because the revised language in § 7152(a)(1) provides greater specificity on the difference between generic and non-generic language when identifying a purpose.
7152(a)(2) [previously 7152(a)(2)(A)]	654	Comment argues that § 7152(a)(2), previously § 7152(a)(2)(A), introduces a new data minimization standard not found in the CCPA. Businesses should not have to comply with conflicting standards for data	The Agency disagrees with this comment. Civil Code §§ 1798.100(c) and 7002 impose requirements regarding how businesses can process personal information. § 7152(a)(2) provides guidance to businesses that when

		minimization between general CCPA compliance and DPIAs.	identifying the categories of personal information, including sensitive personal information, to be processed, this must include the minimum personal information that is necessary to achieve the purpose of processing consumers' personal information. The risk assessment requirements do not conflict with Civil Code § 1798.100(c) and § 7002, but rather provide clarity about how to identify relevant personal information that complies with those requirements.
7152(a)(2) [previously 7152(a)(2)(A)]	994	Comment suggests that § 7152(a)(2), previously § 7152(a)(2)(A), should allow flexibility in defining "necessary" personal information, especially in contexts like AI model training, where data sufficiency evolves over time. This risks conflict with § 7152(a)(2)(B).	The Agency disagrees with this comment. The recommendation is not necessary, and there is no conflict because businesses are always able to update their risk assessments as they have more information to determine what personal information are "necessary." In addition, § 7152(a)(2)(B) has been removed to simplify implementation for businesses at this time.
7152(a)(2)(B)	1726	Comment recommends striking subsection (a)(2)(B) in its entirety.	The Agency agrees with this comment, to the extent it requests removal of this subsection. The Agency has removed § 7152(a)(2)(B) to simplify implementation for businesses at this time.
7152(a)(2)(B)	1879	Comment states that the requirements for businesses to identify the actions they plan to take to "maintain the quality of personal information processed" by the ADMT is redundant with the statute's "accuracy" requirement in Civil Code § 1798.106. It should be struck entirely.	The Agency disagrees with this comment. The Agency does not believe that the requirement to identify actions regarding maintaining the quality of personal information is redundant. Nevertheless, the Agency has removed this requirement to further simplify implementation for businesses at this time.
7152(a)(3)	1727	Comment recommends editing subsection (a)(3) to read: "The business must identify the relevant operational elements of the processing activity, which may include…."	The Agency disagrees with this comment. The operational elements identified in subsection (a)(3) are all necessary to conduct a risk assessment, so comment's suggestion to include "relevant" is unnecessary. The Agency also revised the regulation to further clarify that the business must identify and

			document in a risk assessment report the specific operational elements of its processing.
7152(a)(3)	1860	Comment argues that the requirement to identify all technology used in the processing is overly broad. Comment suggests an approach similar to Colorado's, where disclosure is context-specific and more flexible.	The Agency disagrees with this comment. The regulations are not overly broad and are consistent with Colorado's requirements. Nevertheless, the Agency has removed the requirement regarding technology to further simplify implementation for businesses at this time.
7152(a)(3)(B)	1728	Comment recommends editing subsection (a)(3)(B) to read: "An estimate of how long the business will retain the personal information, and any criteria used to determine that retention period."	The Agency disagrees with this comment. The regulation is clear about what information must be identified and has been revised to provide further clarity to businesses regarding how to identify the information for this operational element. Comment's recommendation is less effective than the regulation, because it assumes that the business will use the same retention period for each category of personal information, which may not be the case for a given processing activity.
7152(a)(3)(B)	995	Comment seeks revisions to § 7152(a)(3)(B) to ensure flexibility in retention periods, considering evolving legal and regulatory requirements and the dynamic and sometimes conflicting nature of data retention obligations.	The Agency agrees in part with this comment. The regulation has been revised to provide further clarity about what retention information is necessary to conduct a risk assessment. The Agency disagrees in part with this comment, to the extent it suggests that the regulation conflicts with businesses' other data retention obligations. The comment has not identified any data retention obligations that conflict or overlap with the regulation.
7152(a)(3)(D)	1107	Comment cites example regarding identifying the approximate number of consumers whose personal information the business seeks to process. Comment argues that this is unclear and may be difficult to comply with when businesses enter new markets or	The Agency disagrees with this comment. The regulation is clear about what information must be identified and has been revised to provide further clarity to businesses regarding how to identify the information for this operational element. The regulation is not

		expand their offerings. Comment requests additional guidance or flexibility regarding compliance.	difficult to comply with, because businesses may update the risk assessment as they obtain new information.
7152(a)(3)(D)	1444	Comment recommends deleting requirement to include approximate number of consumers whose PI the business seeks to process.	The Agency disagrees with this comment. Identifying the approximate number of consumers whose personal information the business plans to process is necessary to identify the risks and benefits of a given processing activity.
7152(a)(3)(E)	1729	Comment recommends striking subsection (a)(3)(E) in its entirety.	The Agency disagrees with this comment. Identifying what disclosures that a business has made, or plans to make, about the processing of personal information and how they were, or will be, made is necessary to identify risks to consumers' privacy, such as whether the processing is consistent with their reasonable expectations. The regulation has also been revised to further simplify implementation for businesses at this time.
7152(a)(3)(F)-(G)	1730	Comment recommends striking subsections (a)(3)(F) and (G) and replace with: "the technology, service providers, and contractors to be used in the processing."	The Agency disagrees with this comment. Identifying the names or categories of relevant service providers, contractors, or third parties and the purpose for making personal information available to them is necessary to identify risks to consumers' privacy, such as to assess the risk of unauthorized access. Similarly, identifying the logic of the ADMT and how an output will be used is necessary to identify risks to consumers' privacy, such as ensuring the ADMT is working in a way that is accurate and nondiscriminatory. These requirements are also consistent with approaches in other jurisdictions, such as Colorado. Further, the Agency has revised the regulations to simplify implementation for businesses at this time, including deleting language regarding "technology."

DRAFT

7152(a)(4)-(a)(6)	1731	Comment recommends editing subsection (a)(4) to use the word "expected," delete the word "specifically," and delete the last sentence regarding profit. Comment also recommends edits to subsection (a)(5) to similarly remove requirement regarding specificity, add the word "known," and delete portions of the requirement regarding criteria. Lastly, comment recommends deleting second sentence of subsection (a)(6) and striking subsection (a)(6)(B).	The Agency disagrees with this comment. The Agency has revised the regulation to provide additional clarity to businesses regarding how to identify relevant benefits, negative impacts, and safeguards. This includes guidance regarding specifically identifying benefits. Comment's recommendation to use "expected" and "known" is not necessary to identify benefits and negative impacts. Additionally, the Agency also revised the regulation to further simplify implementation for businesses at this time, including deleting subsection (a)(6)(B). The Agency also removed language regarding expected profit.
7152(a)(4)	653	Comment opposes the requirement for businesses to disclose anticipated profits from data processing in DPIAs. Comment argues that this could lead to anti-competitive consequences.	The Agency disagrees with this comment. Risk assessments are submitted to the Agency, so it is unclear why identifying this information would cause anti-competitive consequences. Nevertheless, the Agency has removed the language regarding anticipated profits. The Agency also clarified that a business must not identify a benefit in generic terms and provided guidance on how to identify a benefit in non-generic terms.
7152(a)(4)	996	Comment suggests clarifying that not all processing benefits every stakeholder, advocating for a revision in § 7152(a)(4).	The Agency agrees with this comment. The regulation has been revised to clarify that benefits may be applicable to different categories of stakeholders.
7152(a)(4)	1125	Comment asserts that the requirement that businesses explicitly describe the benefits of data processing is too restrictive, limiting companies from using general terms such as "improving our service" and forcing them to disclose proprietary business details.	The Agency disagrees with this comment. The regulation is clear and has been revised to add further clarity regarding how to identify a benefit in non-generic terms. In addition, when providing this required information, the CCPA states that a business is not required to divulge trade secrets.
7152(a)(4)	1445	Comment recommends deleting example in subsection.	The Agency disagrees with this comment. Identifying a benefit in non-generic terms is necessary to ensure that

			businesses can meaningfully identify the benefits of a given processing activity. The regulation has been revised to provide further clarity regarding how to identify a benefit in non-generic terms. The Agency has also removed the language regarding anticipated profits.
7152(a)(5)	103	Comment suggests listing various risks, including privacy violations, economic harms (e.g., termination, wage reductions), physical harms (e.g., injuries from automated productivity quotas), and psychological harms (e.g., stress from workplace surveillance), because current regulations do not sufficiently specify the potential harms workers may face from ADMTs beyond hiring discrimination.	The Agency disagrees in part with this comment. The regulations provide clarity and guidance about potential privacy harms. In addition, because the regulations are intended to apply to variety of industries and contexts, the harms identified are a nonexhaustive list. Businesses may consider other negative impacts to consumers. The Agency does not believe additional examples are necessary at this time.
7152(a)(5)	1929	Comment states that it is unreasonable to ask businesses to identify the impacts of something which 10 well-intentioned people would describe differently. As worded, these regulations ask them to describe everything. Comment suggests saying "use reasonable efforts to identify potential negative impacts…." In § 7152(a)(5)(C), comment suggests using the phrase "privacy or security choices" instead more open-ended language about the processing of personal information.	The Agency disagrees with this comment. The recommendation to use the language "reasonable efforts" does not provide sufficient clarity regarding what is expected of a business when identifying negative impacts. Additionally, impairing consumers' control over their personal information is not limited to making privacy or security choices. Although the Agency believes the regulation is clear, it has been revised to further simplify implementation for businesses at this time.
7152(a)(5)(B), (a)(6)(B)	1446, 1930	Comment recommends deleting the subsections regarding discrimination. Comment argues that discrimination is against the law in the first place, so the Agency should presume businesses are not doing it. And if they were, they businesses would not admit to it on paper. Comment does not think these kinds of violations are privacy violations. CPRA is a privacy statute and this requirement for businesses to become civil rights enforcers is not supported by	The Agency disagrees with this comment. Discrimination is a privacy harm. This is consistent with both the text and purposes of the CCPA and with other privacy frameworks. Risk assessments enable businesses to identify privacy harms, including discriminatory harms before initiating the processing activity. This protects consumer privacy by ensuring they are not subject to unlawful discrimination that a business had not previously identified and safeguarded

		statute. Also, businesses should not have to evaluate whether ADMT does not discriminate. This is asking too much of businesses that buy off-the-shelf software that incorporates some aspect of ADMT. Perhaps this could be limited to "evaluate whether the technology hurts security" but it should not mention ADMT.	against. However, to simplify implementation at this time, the mandatory safeguards in § 7152(a)(6) are now provided as guidance for businesses to consider in their risk assessments.
7152(a)(5)(D)	1447	Comment recommends deleting example in subsection.	The Agency disagrees with this comment. The example provides guidance to businesses regarding how to identify potential privacy harms regarding coercing or compelling consumers into allowing the processing of their personal information.
7152(a)(5)(E)	1448, 1931	Comment recommends deleting subsection regarding media consumption, or deleting the phrase "in a manner that chills or deters their speech, expression, or exploration of ideas." Comment asks how a business is supposed to determine if someone finds a disclosure chilling. The Agency is a privacy agency and now it is proposing that businesses monitor their consumers' beliefs to determine how said consumers feel about freedom of expression. This is far away from "risks to consumer's privacy and security" and courts will consider this regulatory overreach.	The Agency agrees in part with this comment, to the extent the comment requests deleting this subsection. The Agency deleted the subsection because it is already addressed via the privacy harm of impairing consumers' control over their personal information identified in § 7152(a)(5)(C).
7152(a)(5)(E) [previously 7152(a)(5)(F)]	343, 608, 1053, 1932	Comment objects to the inclusion of "economic harms" (such as charging higher prices or lower compensation) as a privacy risk, arguing that they do not fall under the Agency's consumer privacy mandate. They recommend removing these references or limiting it to "economic harms from the unauthorized access to consumers' personal information." Comment thinks that these examples will be litigated and does not think that the examples have anything to do with privacy or security, which is the	The Agency disagrees with this comment. Privacy risks include economic harms to consumers, and the regulation provides examples as guidance of how processing of personal information can cause these harms. In addition, the Agency has revised the regulation to state that this is a nonexhaustive list of harms that businesses may consider when identifying privacy risks to consumers. This provides both clarity and flexibility for businesses.

		subject of the risk assessment language in the statute.	
7152(a)(5)(G), (H) [previously 7152(a)(5)(H), (I)]	1449, 1450	Comment recommends deleting some of the examples in these subsections.	The Agency disagrees with this comment. The examples provide guidance to businesses regarding how to identify potential privacy harms regarding reputational and psychological harms. However, the Agency revised the regulation to further simplify implementation at this time.
7152(a)(5)(G) [previously 7152(a)(5)(H)]	1933	Comment thinks that "would" should be "could" because it is so subjective. Also, the example needs to be cleaned up because the way it's worded it implies that disclosing "a consumer's sexual or other preferences in a partner" is a harm when that's exactly what dating apps do and what consumers want them to do.	The Agency agrees with this comment, to the extent it requests additional clarity. The Agency has revised the regulation to use the word "could" and to clarify the example regarding a consumer's sexual or other preferences.
7152(a)(5)(G) [previously 7152(a)(5)(H)]	1934	The Agency should clarify this language: "a business stating or implying that a consumer has committed a crime without verifying this information." Comment says that if FB shows a post by a consumer alleging another consumer committed a crime, FB is not responsible for that post because of Section 230. The regulations should steer well clear of the Section 230 bright line by clarifying this language.	The Agency disagrees with this comment. Privacy harms include disclosing inaccurate information about the consumer, which is supported by both the CCPA's right to correct and case law. However, the Agency has revised the regulation to simplify implementation at this time.
7152(a)(5)(H) [previously 7152(a)(5)(I)]	405, 747, 1935	Comment states that § 7152(a)(5)(H), § previously 7152(a)(5)(I), is subjective or impractical since businesses lack the expertise to assess mental health impacts of the average consumer — this is better suited for medical professionals. The Agency should delete the examples listed in the subsection. The Agency should not specify these different harms and imply that a business must consider them all.	The Agency disagrees with this comment. Privacy risks include psychological harms to consumers, and the regulation provides examples as guidance of how processing of personal information can cause these harms. In addition, the Agency has revised the regulation to state that this is a nonexhaustive list of harms that businesses may consider when identifying privacy risks to consumers. This provides both clarity and flexibility for businesses.

7152(a)(6)	655	Comment argues that § 7152(a)(6) implicates First Amendment concerns, referencing the Ninth Circuit Court of Appeals decision in *NetChoice v. Bonta*. The Bonta analysis applies, because the DPIA sets forth in § 7152(a)(5) criteria that clearly reveal what the Agency considers a negative privacy harm, and then mandates in §7154 that a business not process personal information for "any processing activity" that presents a "significant risk" (in the Agency's judgment) to consumer privacy if the DPIA identifies that the risks outweigh the benefits. As such, these provisions invite litigation that follow on the *NetChoice v. Bonta* path. Comment urges the Agency to remove these provisions.	The Agency disagrees with this comment. The Agency does not believe the regulations violate the First Amendment. Further, the regulations implement a state law that tasks the Agency with its implementation. The Agency does not have the authority to deem a state law invalid or in conflict with constitutional provisions. The CCPA also directs the Agency to require businesses whose processing of consumers' personal information presents significant risk to their privacy to conduct a risk assessment and submit it to the Agency on a regular basis. (Civ. Code § 1798.185(a)(14).) The regulations are within the Agency's authority and further the intent and purposes of the CCPA. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, it is required to issue regulations and impose certain requirements. Nevertheless, §§ 7152 and 7154 have been revised to further simplify implementation at this time, and to clarify the goal of a risk assessment as stated in the statute.
7152(a)(6)(A)	997	Comment worries that referencing external parties in § 7151(b) may imply mandatory consultation, recommending broader phrasing. Comment recommends that the reference to § 7151(b) be removed and revising § 7152(a)(6)(iii) to read as follows: "(iii) Consulting external parties and resources to ensure that the business maintains current knowledge of emergent privacy risks and countermeasures; and using that knowledge to identify, assess, and mitigate risks to consumers' privacy."	The Agency disagrees with this comment. The regulation is clear that it is a safeguard businesses may consider, and § 7151(b) is referenced to provide guidance on the types of external parties a business may consult.
7152(a)(6)(B)	259	Comment argues that the proposed regulations lack specific guidance on acceptable methodological	The Agency disagrees with this comment. The regulation provides a clear performance standard for

		standards for assessing ADMTs' potential discriminatory outcomes.	businesses that is adaptable to a variety of industries and contexts. However, the Agency revised the regulation to further simplify implementation for businesses at this time, so that a business can consider as a safeguard whether to implement policies, procedures, and training to ensure that the ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics.
7152(a)(6)(B)	843	Comment suggests that ADMTs are frequently based on processes or algorithms that can learn. As a result of this learning, they are susceptible to deviation from their original Scope, Nature, Context, and Purpose and thus need continuous monitoring. It is the risk of these types of deviations that suggest that a regular consideration of the DPIA should be conducted.	The Agency agrees with this comment, to the extent it supports conducting risk assessments for certain uses of ADMT that present significant risk to consumers' privacy. With respect to comment's point regarding continuous monitoring, § 7155 contains timing requirements to ensure that risk assessments are updated when there is a material change in the processing activity or every three years.
7152(a)(6)(B)(i)	959	Comment states that the regulations require businesses using ADMT for profiling to evaluate that their technologies "do not discriminate based upon protected classes." However, this language is overly broad and could prohibit lawful and beneficial distinctions, such as age-based marketing for retirement services. The Agency should clarify that businesses must ensure ADMT does not unlawfully discriminate, aligning with existing California anti-discrimination laws.	The Agency agrees in part with this comment, to the extent it seeks to clarify that unlawful discrimination is a privacy harm. To simplify implementation for businesses at this time, the Agency has revised the references to discrimination in § 7152 to clarify that it is "unlawful discrimination."
7152(a)(8)-(9)	926, 1452	Comment argues that §§ 7152(a)(8)-(9)'s requirement to disclose employee names raises confidentiality concerns. Comment suggests deleting the requirement to include names and positions of individuals responsible for review and approval of the risk assessment.	The Agency disagrees with this comment. Identifying the individuals who contributed to, reviewed, or approved the risk assessment is necessary to ensure accuracy and accountability.

7152(a)(8)	1626	Comment asserts that the term "contributors" is vague, and clarification is needed.	The Agency disagrees with this comment. The term "contributor" is reasonably clear based on the plain meaning of the word. However, the Agency has revised the regulation to further clarify which individuals must be identified as part of the risk assessment.
7152(a)(9)	406, 748	Comment argues that § 7152(a)(9) is not feasible for large organizations where decisions are made collaboratively across departments. Decisions in such organizations are typically collaborative and cross-functional, making this requirement unrealistic. Comment recommends removing reference to single individual.	The Agency disagrees with this comment. The requirement is feasible. Nonetheless, the Agency has revised § 7152(a)(9) to clarify that an individual with authority to participate in deciding whether the business will initiate the processing must review and approve the assessment.
7153	1732	Comment recommends editing this section to add in language regarding the nature of processing and information available to the business, the training of ADMT using personal information, and concepts of reasonable necessity and relevance. Comment also suggests removing references to persons, AI, and plain language.	The Agency disagrees with this comment. The recommended language is less effective than the regulation, because it would limit the disclosure requirements for businesses making ADMT available to other businesses. Further, the Agency has revised § 7153 to focus on businesses making ADMT available to others to make a significant decision and delete what was originally proposed as § 7153(b), so comment's recommendations are not necessary at this time.
7153(a)	822	Comment affirms that transparent risk assessment, including disclosure of residual risk, enhances risk management for downstream deployers and consumers. Comment believes that this requirement should be applicable to all ADMT providers, deployers and AI subjects (persons impacted by an ADMT or AI) and not just as to those subject to a risk assessment per § 7150.	The Agency disagrees with this comment. The CCPA requires that businesses conduct a risk assessment. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. To the extent a provider or deployer is a business for purposes of the CCPA and plans to engage in any of the activities in § 7150(b), it must conduct a risk assessment.
7153(a)	1108	While comment agrees with the principle of ensuring that there is a robust framework for developing risk assessments throughout the data supply chain, as	The Agency agrees in part with this comment, to the extent it supports § 7153's requirements to ensure risk assessments are conducted with accurate information.

		written, this provision presents ambiguity as to the specific information that a business making ADMT or AI should provide to the partner business. Therefore, comment recommends that Agency provide additional clarity within the regulations or via subsequent guidance upon finalization of the rule.	However, the regulation is clear about the necessary facts to conduct a risk assessment, as well as what information is to be provided. Nevertheless, the Agency revised the regulation to provide further clarity that this means the information that is available to the business. The regulation is reasonably clear based on the plain meaning of the words. The Agency believes that no further clarification is needed at this time.
7153(b)	823	Comment affirms that transparency requirements afforded upstream parties to downstream parties and AI subjects results in a reduction in harms and more informed use.	The Agency agrees in part with this comment, to the extent that it states that § 7153(b) provides benefits to businesses and consumers. Nevertheless, to simplify implementation for businesses at this time, the Agency has removed § 7153(b).
7154	108, 975, 1074, 1747	Comment advocates for strengthening the Agency's authority to act on risk assessments, ensuring that identified risks lead to meaningful regulatory enforcement and oversight. Comment supports § 7154 and calls for giving the Agency explicit authority to challenge businesses' risk assessments if they fail to demonstrate that the benefits of data processing outweigh the privacy risks. Comment argues that the current framework lacks a clear enforcement mechanism or allows businesses to self-certify their compliance, limiting the Agency's ability to intervene. Comment suggests adding language to require businesses to provide additional documentation if the CPPA finds deficiencies, and if necessary, hold a hearing to determine whether processing should be restricted or prohibited. Comment also states that the Agency should have explicit authority to review assessments, require corrective action, and prohibit processing if consumer risks outweigh benefits.	The Agency disagrees with this comment. Businesses are not allowed to self-certify compliance. They must comply with the requirements set forth in Article 10. Additionally, comment's suggested language is not necessary. As with other violations of the CCPA, the Agency has enforcement authority if a business is not complying with the law. Further, § 7154 has been revised to clarify the goal of the risk assessment, which provides clear guidance to businesses and is consistent with the CCPA's plain language.

7154	276, 340, 341, 342, 343, 344, 346, 407, 749, 776, 1026, 1091, 1109, 1549, 1601, 1627, 1834, 1861, 1896	Comment states that the proposed provision prohibiting processing if privacy risks outweigh the benefits is too broad, is impermissibly vague, violates due process due to indiscernible standards, is subjective, goes beyond the statutory requirement to evaluate risks, and is beyond the Agency's authority to require. It goes beyond the scope of other AI regulations like the EU AI Act, which restricts specific uses rather than broadly prohibiting activities. It also would discourage innovation and lead businesses to take either overly cautious or risky approaches to compliance, which could lead to withholding products from consumers. Businesses lack clear standards for compliance and may face arbitrary or inconsistent enforcement. The Agency's broad definition of "significant risks" and subjective privacy harms further complicate compliance. Comment argues that the CCPA envisions risk assessments as a tool to encourage companies to mitigate risks, not as a justification for prohibiting practices. Comment argues that the Agency should defer to the reasonable judgment of the business. Comment also raises concerns in the HR context, because benefits can be long-term, qualitative, and difficult to quantify, and the regulation lacks guidance on how to compare these factors. Comment recommends removing this provision or narrowing the provision to a harm-based test or to prohibit processing that causes substantial and unavoidable harm to consumers when the harm is not outweighed by benefits. Comment suggests modifying the provision by requiring that benefits significantly outweigh privacy risks, to identify prohibited ADMT use and ensure corrective measures. Comment requests the Agency acknowledge the	The Agency disagrees with this comment. The language in § 7154 as revised is the CCPA's explicit statutory requirement. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. § 7154, as revised, provides a clear and flexible standard that applies to a variety of contexts and industries. The risks provided in § 7152 are guidance for businesses to consider when conducting the risk assessments, and provide additional clarity about different privacy harms. Further, the Agency must use the same requirements in Article 10 to assess a business's compliance, which provide appropriate parameters for the Agency's discretion.

		benefit-risk evaluations in risk assessments and recommends a mechanism for businesses to seek regulatory guidance in ambiguous cases. Comment requests additional guidance or clarification, such as whether safeguards are explicitly part of the balancing test. Comment suggests using the Colorado regulations or the Virginia law as a model.	
7155	927	Comment believes that § 7155's requirements of updates every three years and upon material changes in data processing could discourage innovation. A more flexible approach, like Colorado's law, should be adopted, requiring reviews based on the sensitivity of data and risk level rather than a fixed schedule. If retained, "material change" should be defined as one that is "materially adverse to the consumer's privacy."	The Agency disagrees with this comment. The update requirements are necessary to ensure that risk assessments remain accurate, particularly after a material change to the processing. This is consistent with both Colorado's and GDPR's approach, which require or provide guidance to periodically review risk assessments. Comment's recommendations are less clear than the proposed regulation, because they do not provide sufficient clarity on when changes are "materially adverse" to privacy nor what level of sensitivity or risk level triggers an update. By contrast, the regulations provide a clear standard regarding timing for updating risk assessments.
7155	1733	Comment recommends editing § 7155 to remove requirement to review risk assessments at least once every three years, and to instead use an "as appropriate standard." Comment also recommends revising definition of material change to include a standard of "significance" and changing the definition so it is nonexhaustive.	The Agency disagrees with this comment. Comment's recommended language is less effective than the regulation because it does not require consistent reviews of the risk assessment. It also provides less clarity to businesses about when risk assessments must be updated or what constitutes a material change.
7155(a)	168, 1157, 1489	Comment suggests that the requirement in § 7155(a)(3) to "immediately" update risk assessments where there is a "material change" is unrealistic, given that a proper risk assessment requires careful collection and assessment of information. A standard requiring a business to update a risk assessment	The Agency disagrees with the comment that it is unrealistic to require immediate updating of risk assessments when there is a material change to the processing. However, § 7155(a)(3) has been revised to give businesses up to 45 days to update their risk assessments when there is a material change. This

		within a reasonable period of time, or within a period of business days, would be more realistic given the time and effort that goes into properly conducting a risk assessment. Comment states that the language should specify that material changes related to the processing activity should be likely to have an impact on consumer privacy to result in an update to the risk assessment. In addition, businesses should be allowed to update a risk assessment within a reasonable time instead of immediately.	balances protections for consumer privacy with providing flexibility for businesses in meeting their compliance obligations.
7155(a)(2)	1453	Comment suggests deleting requirements to do a risk assessment every three years.	The Agency disagrees with this comment. This regulation is necessary to ensure that risk assessments address risks to consumers' privacy throughout a processing activity's lifecycle and do not reflect out-of-date information. This is consistent with approaches taken in other jurisdictions, such as the EU and Colorado.
7155(a)(3)	202	Comment suggests revision as follows: "Notwithstanding subsection (a)(2) of this section, a business must update a risk assessment whenever there is a material change relating to the processing activity. A change relating to the processing activity is material if it diminishes the benefits of the processing activity as set forth in section 7152, subsection (a)(4), creates new negative impacts or increases the magnitude or likelihood of previously identified negative impacts as set forth in section 7152, subsection (a)(5), or diminishes the effectiveness of the safeguards as set forth in section 7152, subsection (a)(6), in each case as material to the benefits, impacts, or effectiveness of the safeguards. Material changes may include, for example, material changes to the purpose of the processing; material	The Agency disagrees with this comment. The Agency revised § 7155(a)(3) to clarify the standard for a material change: whether it creates new negative impacts or increases the magnitude or likelihood of previously identified negative impacts or diminishes the effectiveness of safeguards. The proposed revision is less clear than the regulation. The comment's additions of "in each case as material to the benefits, impacts, or effectiveness of the safeguards" and the word "material" in the second paragraph do not provide additional clarity or guidance to businesses about when a change is material. Similarly, the proposed deletion of the last phrase would make how to identify a material change less clear. These recommendations are also not as effective as the regulations in protecting consumer

		changes to the minimum personal information necessary to achieve the purpose of the processing; or material changes to the risks to consumers' privacy."	privacy because they would minimize the situations that require an update to the risk assessment.
7155(a)(3)	1352	Comment appreciates the value in updating risk assessments following a material change, provided that the scope of "material change" is amended to align with the longstanding definition of the term. The regulations should adopt the FTC's definition of materiality – i.e., whether it would affect a consumer's decision to interact with the product or service. The draft regulations define "material" in a way that would include an update beneficial to the consumer, which, in practice, would delay benefits to the consumer until documentation could be finalized. Also, the draft regulations should not require "immediate[]" updates to risk assessments because good faith efforts to comply could result in hurried updates that do not address significant risks to privacy intended by the statute.	The Agency disagrees with this comment. The regulation provides a clear definition of what is a material change, with guidance about what this may include. This is a clearer standard tied to the risk assessment requirements than the standard proposed by the comment. The FTC's definition of "materiality" is not tied to risk assessments, but to disclosures to consumers, which is a different context and set of requirements. The regulations have also been revised to give businesses up to 45 days to update their risk assessments when there is a material change and to remove the diminishing benefits from the definition of material change. This provides a clear standard and additional flexibility for businesses to update their risk assessments.
7155(b) [previously 7155(c)]	167, 408, 611, 750, 1025, 1455, 1456	Comment suggests that the Agency should clarify that risk assessments are required only for new or genuinely materially different processing activities. The requirement to conduct risk assessments for all historical activity that would be covered by the rules imposes an enormous compliance burden on businesses without any corresponding consumer benefit. Comment states that the retroactive requirement and 24-month deadline for completing assessments, such as for ADMT uses, is unrealistic and will strain business operations. The Agency should limit requirements to future activities to reduce unnecessary burdens, and/or reasonable limits	The Agency disagrees with this comment. The regulations do not require retroactive assessments but do require a risk assessment for processing that presents a significant risk to consumers' privacy after the effective date of these regulations. In addition, the regulations provide additional time to conduct risk assessments for these processing activities to lessen the compliance burden on businesses. This approach benefits both businesses and consumers, by balancing flexibility for businesses to come into compliance with ensuring privacy protections for processing that presents significant risk to privacy.

		should be set for the lookback period to exclude outdated rules. Comment also recommends stating risk assessments only apply to activities involving the processing of personal information and that were initiated after this Article enters into effect.	
7155(b) [previously 7155(c)]	203	Comment suggests revision as follows: "For any processing activity identified in section 7150, subsection (b), that the business initiated prior to the effective date of these regulations and that continues after the effective date of these regulations, the business must conduct and document a risk assessment in accordance with the requirements of this Article where there is a material change to the data processing."	The Agency disagrees with this comment. The recommendation is not as effective as the Agency's language in § 7155(b), previously § 7155(c), which requires a risk assessment for processing that presents a significant risk to consumers' privacy after the effective date of these regulations. If comment's suggestion was adopted, it would result in a disparity in consumer protections based solely on when the processing activity was first initiated by the business, even if the processing is taking place at the same time with information from the same consumer. The regulations also provide businesses with additional time to conduct risk assessments for these processing activities, to lessen the compliance burden on businesses. Moreover, the proposed revision of "when there is a material change to the data of processing" is not as effective in protecting consumers' information.
7155(c) [previously 7155(b)]	1454	Comment suggests deleting requirement to retain risk assessments for at least five years.	The Agency disagrees with this comment. The regulation is necessary to specify the duration that businesses must retain risk assessments.
7156	277, 1604, 1628, 1918	Comment contends that the provision creates overly broad requirements for conducting risk assessments, which do not align with the more tailored standards found in other state privacy laws. The draft regulations also introduce a vague requirement that a risk assessment conducted under other laws must cover a comparable set of processing activities with similar	The Agency disagrees with this comment. § 7150(b) provides clear guidance on what processing activities present significant risk to consumers' privacy and therefore require a risk assessment. These thresholds are also consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clear

DRAFT

		risks to consumers' privacy. This creates confusion, as businesses cannot determine what constitutes "similar risks" without first conducting a risk assessment, defeating the intent of the provision. Comment recommends working with other regulators to promote interoperability, such as a list of acceptable assessments or templates and tools to help businesses navigate across jurisdictions, because risk assessments can be resource-intensive. Comment also urges aligning requirements with those in other states, which limit assessments to sensitive data or profiling with foreseeable risks.	guidance to businesses about what is in scope. In addition, § 7156 uses the same standard as Colorado's regulations for comparable sets of processing activities and enables businesses to leverage existing compliance processes for Colorado's and other jurisdictions' requirements for the CCPA.
7156(b)	204, 809, 1116, 1292, 1457, 1550, 1835	Comment states that this requirement is too rigid or is problematic because a company cannot determine whether a given processing activity presents a "similar risk" without first conducting a new risk assessment, creating a circular burden. Comment also states that the proposed rules should be revised to align the required content for risk assessments more closely to the statutory text and to promote interoperability. Comment suggests allowing businesses to use other DPIAs or data protection assessments, such as those under GDPR or other state laws, to comply with the CCPA. They propose revisions, such as using a reasonableness standard, to promote interoperability and consumer protections.	The Agency agrees in part with this comment, to the extent it supports businesses' use of existing assessments under GDPR or other state laws to comply with the CCPA's requirements. The regulation has been revised to clarify that a business may use a risk assessment that it has already done, provided that it contains all the information required by California, either on its own or by supplementation, to comply with § 7152; the Agency has also included an example. However, the language suggested by the comment does not clearly convey to businesses when a risk assessment conducted to comply with another law or regulation can be used meets the requirements of the CCPA. By contrast, the regulation is clear about what a business must do if the risk assessment does not include the required components in § 7152. The regulations are consistent with the CCPA's requirements for risk assessments and are necessary to ensure businesses conduct risk assessments appropriately.
7156(b)	751	Comment recommends asking for an explicit exemption for federally regulated financial	The Agency disagrees with this comment. § 7156(b) provides a clear standard for businesses about how

		institutions by substituting compliance with existing risk assessment requirements for compliance with the CPPA's requirements.	they can use existing compliance processes to conduct a risk assessment under the CCPA. Comment also provides no basis to justify an entity level-exemption for financial institutions from the risk assessment requirements or that the risk assessments they conduct are comparable to the requirements in Article 10. To the extent they are comparable, § 7156(b) enables businesses to use those risk assessments.
7157	473, 474, 530, 648, 709	Comment opposes the requirement in § 7157 that DPAs must be filed annually. Instead, comment argues that businesses should only need to make DPAs available upon request. Comment cites concerns about excessive documentation, confidentiality risks, and misalignment with global privacy norms and other state laws. Comment argues that the regulations ignore best practices of other jurisdictions. If filing is required, comment requests confidentiality protections due to the sensitive nature of the information contained in DPAs and an exemption from public disclosure under the Public Records Act. Other states only require assessments to be disclosed during investigations and exempt them from public records requests to protect confidentiality. Comment urges the Agency to align its approach with other jurisdictions. Comment also suggests requiring attestations of compliance, such as under GDPR, or exempting complies subject to similar attestations, because this would otherwise create significant operational, legal, and security issues. Comment raises concern about a honeypot for organizations seeking to attack regulated entities. Any requirement to submit a risk assessment should not be done through an online portal due to potential confidentiality breaches and the possibility that	The Agency disagrees with this comment. Businesses must submit risk assessments to the Agency pursuant to the CCPA. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The regulations balance providing flexibility to businesses while ensuring that they provide necessary information to the Agency. This means, on an annual basis, providing certain risk assessment information to the Agency, and providing risk assessment reports upon request. Additionally, whether information in the Agency's records is subject to public disclosure depends on the specific information and whether an exception to the Public Records Act applies. Businesses will annually submit risk assessment information via the Agency's website, which the Agency has determined provides appropriate security.

		individuals will submit the state equivalent of FOIA requests. The Agency should be able to request copies through a secure channel, which is similar to market conduct review conducted by the California Department of Insurance.	
7157	205, 252, 403, 1102, 1354, 1381, 1383, 1490, 1551, 1603, 1630, 1736, 1738, 1836	Comment suggests that the Agency should (consistent with the grant of rulemaking authority in the CCPA) expressly clarify that the regulations do not require businesses to divulge trade secrets or privileged information and are exempt from public disclosure. Comment also raises concerns about requiring submissions in employment contexts, which could expose trade secrets and confidential business data. The regulations should recognize that a business can withhold from submission trade secret and privileged or business sensitive information in a risk assessment or otherwise set forth protections when submitting risk assessments upon request to prevent the public disclosure of such information and the waiver of related privileges. Comment states that this is consistent with other states' approaches and with the Age Appropriate Design Code.	The Agency disagrees with this comment. The CCPA already states in Civil Code § 1798.185(a)(14)(B) that "[n]othing in this section shall require a business to divulge trade secrets." The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The risk assessment regulations also do not require submission of attorney-client privileged information. Additionally, whether information in the Agency's records is subject to public disclosure depends on the specific information and whether an exception to the Public Records Act applies.
7157	278, 279, 347, 609, 610, 891, 928, 1092, 1156, 1172, 1314, 1324, 1353, 1381,	Comment states that this provision is overly burdensome, excessive, and unnecessary, because the regulation offers no clear consumer benefit while imposing significant demands on businesses. This requirement also deviates from the approach taken by other state privacy laws, raises compelled speech concerns, may reduce privacy protections as businesses prepare assessments in a way that is legally protective rather than focused on risk-benefit balancing, and could expose businesses to security risks and undermine competitiveness. Comment	The Agency agrees in part with this comment, to the extent it requests additional time to submit risk assessment reports to the Agency. Although the proposed 10-day submission requirement was not unduly burdensome, the Agency extended the timeline to 30 calendar days to further simplify implementation for businesses at this time. The Agency otherwise disagrees with this comment. The CCPA requires that businesses submit risk assessments to the Agency. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The submission

	1383, 1551, 1630, 1734, 1735, 1738, 1836, 1891, 1996, 2001	suggests using a more flexible approach focusing only on high-risk activities, such as selling sensitive data or decisions that result in legal or similarly significant effects, or where risks are unmitigated; aligning risk assessment requirements with those of other states; or using a three-year update cycle and only requiring updates within 30 days of changes. Additionally, comment recommends exceptions for employment-related decisions, as this information is often confidential or involves trade secrets. Comment states that the requirements to submit risk assessments annually and within ten days upon the Agency's request are overly burdensome and inconsistent with other state privacy laws. Comment suggests a more flexible approach, such as submitting certifications only, submitting assessments upon request or as part of an investigation in a confidential and privileged manner with a certification done in advance, allowing a 30-day response window, and/or deferring to the obligations in § 7157(d) after the initial submission. A 30-business day response window provides companies time to review, ensure accuracy, and certify the assessment before submission or allow for coordination internally, and would align with other state laws. Comment also requests a more realistic timeline to update risk assessments in response to material changes. Comment also suggests deleting many requirements in this section.	requirements have been revised to further simplify implementation for businesses at this time. Deferring obligations in § 7157(d) is not necessary because it only requires submission of risk assessment reports that businesses must have already completed. In addition, an annual submission ensures continual compliance with the risk-assessment regulations and promotes consistency across the risk-assessment and cybersecurity-audit regulations, the latter of which similarly require completion on an annual basis. Each of the processing activities for which a business must conduct a risk assessment present significant risk to consumers' privacy, so comment's recommendation to only focus on high-risk activities is duplicative. With respect to employment-related decisions, an exemption is not necessary. The CCPA already states in Civil Code § 1798.185(a)(14)(B) that "[n]othing in this section shall require a business to divulge trade secrets." The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Expanding this exemption to other employment-related data would not be more effective than the regulation at protecting consumer privacy. With respect to compelled speech, the comment does not explain what its compelled speech concerns are. Nevertheless, the Agency does not believe the regulations raise compelled speech concerns. Further, the CCPA requires submission of risk assessment information to the Agency. Additionally, whether information in the Agency's records is subject to public disclosure depends on the specific information and whether an exception to the Public Records Act applies. With respect to material changes, the timing requirements are not unrealistic. However, the Agency has revised the regulation, so a business has up to 45

			days to update a risk assessment after a material change, to further simplify implementation at this time.
7157	779	Comment suggests that to enhance regulatory enforcement, the final regulations should clarify steps the Agency can take when businesses fail to demonstrate that ADMT benefits outweigh risks. A new subsection in § 7157 should authorize the Agency to require additional documentation, hold hearings, and issue orders restricting or prohibiting ADMT use if businesses do not adequately justify their risk assessments.	The Agency disagrees with this comment. Comment's suggested language is not necessary. As with other violations of the CCPA, the Agency has enforcement authority if a business is not complying with the law.
7157	1054	Comment suggests that risk assessments should be required every three years instead of annually to reduce administrative costs. Mandating annual risk assessments and executive certifications imposes significant administrative costs.	The Agency disagrees with this comment. The regulation does not impose significant administrative costs because it requires submission of information that the business already has and an attestation. Nonetheless, to further simplify implementation for businesses at this time, the Agency has revised the annual submission requirements so a business will spend less time preparing the required information.
7157	1749	Comment argues that abridged risk assessments should be made publicly accessible to promote accountability and allow consumers and public interest researchers to evaluate businesses' practices. They assert that transparency would help consumers make informed decisions and serve as an accountability mechanism, especially given limited agency resources. They also highlight that businesses are already protected from being required to reveal trade secrets by statute.	The Agency disagrees with this comment. Under the CCPA, businesses must submit risk assessments to the Agency, not to the public. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Further, the Agency will provide a public report summarizing the risk assessments filed with the Agency, consistent with the requirements of the CCPA. (Civ. Code § 1798.199.40(d).)
7157	1691, 1748, 1973	The abridged risk assessment should include a plain language explanation of the benefit-risk analysis or tradeoffs that the business is already required to	The Agency disagrees with this comment. The Agency has revised the regulation to remove the abridged risk assessment requirements at this time. A business must

		perform under the proposed regulations. This information is essential for the Agency, consumers, and the public to assess whether the business has complied with the law. The compliance burden should be minimal since the business will have already conducted the analysis. Comment recommends restoring this requirement.	still submit relevant risk assessment information and risk assessment reports to the Agency. This balances providing privacy protections for consumers with flexibility for businesses to come into compliance.
7157(b)	872	Comment states that the requirement for submission of risk assessments to the Agency need to include important protections and reasonable parameters.	The Agency agrees in part with this comment, to the extent it states that submission requirements must be reasonable. The Agency disagrees in part with this comment, to the extent it argues that the submission requirements are not reasonable and do not provide sufficient protections for businesses. § 7157 has been revised to further simplify what information must be submitted to the Agency on an annual basis. In addition, risk assessment reports only need to be submitted upon request. These requirements provide flexibility to businesses to come into compliance.
7157(b)	961	Comment states that the regulations provide a 24-month grace period for businesses to conduct risk assessments for existing ADMT processing but require businesses to attest that they only initiated ADMT processing after conducting a risk assessment. This requirement could force businesses that have already been using ADMT to falsely attest that they abstained from processing. The Agency should clarify that the attestation requirement does not apply to businesses using ADMT before the effective date of the regulations.	The Agency agrees with this comment, to the extent it suggests clarifying the relevant time period covered by the attestation. The regulation has been revised so that the attestation in § 7157(b)(5), previously § 7157(b)(1)(B)(iii), applies to relevant processing during the time period of the submission.
7157(b)	1508	Comment states that the current § 7157(b) regulations, requiring only minimal information in abridged risk assessments, do not provide sufficient data for preliminary agency review. The omission of a	The Agency disagrees with this comment. The submission requirements appropriately balance protections for consumers and the burden on businesses to submit the required information. As with

		plain-language cost-benefit analysis undermines the purpose of the assessments. Comment recommends restoring the December 2023 draft language mandating a summary explanation.	other violations of the CCPA, the Agency has enforcement authority if a business is not complying with the law. The Agency considered more extensive requirements for annual submission of risk assessment information, but believes the revised regulations provide appropriate flexibility for businesses to come into compliance at this time.
7157(b)	251, 607, 1052, 1738	Comment recommends simplifying risk assessment requirements to focus only on high-level information that directly benefits risk identification and mitigation. Comment suggests striking §§ 7157(b)(2)-(5) to reduce unnecessary complexity, or striking §§ 7157(b)(2)-(3). If § 7157(b)(2) is retained, only subsection (A) should be kept, and subsections (B)-(D) should be deleted.	The Agency agrees in part with this comment, to the extent it requests further simplifying implementation for businesses. The Agency has removed the abridged risk assessment requirements to simplify implementation at this time. Businesses must submit the risk assessment information set forth in the revised § 7157(b). They must also submit risk assessment reports upon request. The Agency disagrees in part with this comment, to the extent it suggests that the prior requirements were unnecessarily complex or did not focus on relevant information for submission.
7157(b), (c)	1737, 1738, 1892	Comment opposes the requirement to name an individual executive responsible for approving the risk assessment, arguing it could discourage participation due to fear of personal liability. Comment states that certification requirement is excessive, and the requirement for a named executive to certify is burdensome and unnecessary. Comment instead recommends a requirement to submit a written certification on a form provided by the Agency that the business conducted its risk assessment in accordance with the requirements set forth in this Article.	The Agency disagrees with this comment. The certification requirement, including requiring an executive's name, is necessary to ensure accountability at the highest levels of the business when conducting, documenting, and submitting relevant risk assessments to the Agency. These requirements both ensure accountability and simplify implementation for the business in the submission of their risk assessment information.
RAs	101	Comment agrees that pre-use risk assessments are "absolutely critical" to protecting workers and preventing harm when fixes are easier and less costly.	The Agency agrees with this comment and notes comment's support.

		Comment also does not believe requirements are onerous for employers because of the exemption for routine administrative data processing.	
RAs	142, 153, 178, 402, 409	Comment states that federal banking regulations already mandate risk assessments across all business activities, including those involving personal data. Additionally, laws like the Fair Credit Reporting Act ("FCRA") impose specific risk assessment obligations for identity theft prevention. These requirements apply to all data banks handle, making additional mandates unnecessary. Comment suggests that the Agency should provide exemptions for banking organizations that are already subject to federal oversight and federal risk assessment standards. Since no other industry faces comparable regulatory scrutiny, additional state-level rules could create unnecessary burdens without added benefits. In addition, federal regulations governing banking organizations have long ensured the protection of personal information and the overall stability of the financial system. Adding duplicative state-level requirements may divert resources from more effective federal compliance efforts. Comment also recommends that the risk assessment regulations be consistent with existing federal and international standards (e.g., NIST) to ensure harmonization and avoid redundant compliance burdens for federally regulated financial institutions. Comment suggests revising § 7150(b) as follows: "Each of the following processing activities presents a significant risk to consumers except to the extent undertaken in a manner that is subject to examination or supervision by a federal prudential regulator[.]"	The Agency disagrees with this comment. The CCPA applies to "businesses" and does not exempt financial institutions. (*See* Civ. Code §§ 1798.140(d), 1798.145(e).) The CCPA also makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196.) Further, the CCPA includes data-level exemptions for (1) information subject to the Gramm-Leach-Bliley Act and implementing regulations or the California Financial Information Privacy Act and (2) the processing of personal information by certain entities, as long as the activity is regulated by the FCRA, and the processing is as authorized by the FCRA. (*See* Civ. Code §§ 1798.145(d), (e), 1798.196.) The CCPA also directs the Agency to require businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment, and requires that risk assessments be submitted to the Agency on a regular basis. (Civ. Code § 1798.185(a)(14)(B).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The regulations explicitly allow a business to use a risk assessment that it has prepared for another purpose, to comply with in § 7152. (*See* § 7156(b).) Therefore, to the extent a business is already complying with the risk assessment requirements in other laws, it can leverage

			those compliance processes to comply with the regulations.
RAs	165, 1583	Comment suggests that the scope of these regulations should be narrowed (consistent with comparable regimes) to avoid overwhelming the Agency with a deluge of low-quality risk assessments that do not further the goals of the CCPA. Comment recommends tailoring risk assessment obligations for processing activities that present actual significant risk to consumers' privacy and security.	The Agency disagrees with this comment. Each of the thresholds in § 7150(b) presents significant risk to consumers' privacy. These risk assessment regulations are consistent with other risk assessment frameworks, such as those in the EU and Colorado, and further the intent and purposes of the CCPA.
RAs	224, 250, 1115	Comment expresses concern with the approach to risk assessments set out in the regulations. The Agency should require fewer risk assessment materials be submitted to the Agency; define processing that presents a "significant risk" to consumers' privacy in line with other global and state privacy laws, such as the Colorado Privacy Act; and revise the content to be included in risk assessments. As written, the rules significantly expand risk assessments beyond what other states require, including requiring assessments for all behavioral ads.	The Agency disagrees with this comment. Each of the processing activities in § 7150(b) presents significant risk to consumers' privacy. In addition, the submission requirements appropriately balance protections for consumers and the burden on businesses to submit the required information. The requirements are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the intent and purposes of the CCPA and providing clarity to businesses regarding what is required. Further, § 7152 is necessary to provide clarity to businesses regarding what information is necessary to adequately identify the benefits and potential risks of a given processing activity. The regulations have also been revised to further simplify implementation for businesses at this time. For example, the regulations no longer include the separate profiling for behavioral advertising threshold for risk assessments.
RAs	1487	Comment appreciates the 24-month compliance period and reduced duplication for risk assessments but criticizes the inflexibility of requirements.	The Agency agrees in part with this comment, to the extent it supports the regulations' compliance timeline and approach for enabling businesses to use existing risk assessments for compliance. However, the Agency does not believe that the requirements are inflexible.

			The requirements appropriately balance protections for consumers and the burden on businesses to submit the required information. Additionally, the requirements are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the intent and purposes of the CCPA and providing clarity to businesses regarding what is required.
RAs	319	Comment requests clarification on the criteria used to determine when a business's processing of consumer personal information presents significant risk to consumers' privacy that would trigger the requirement to conduct a risk assessment. Guidance is needed on whether a single risk assessment can cover similar processing activities, if separate risk assessments are required for each new or updated use of personal information, the term "material change," and how long to retain assessments after discontinuing a processing activity. Lastly, comment requests clarity on what criteria to use when assessing negative impacts to consumers' privacy.	The Agency disagrees with this comment. § 7150(b) provides clear requirements regarding when a risk assessment must be conducted. Additionally, the standard for using a single risk assessment for multiple purposes is set forth, with examples, in § 7156. Similarly, § 7155 identifies when businesses must be updated, and provides a definition and guidance regarding what constitutes "material change." The regulations also clearly indicate the retention requirements; risk assessments must be retained for as long as the processing continues, or for five years after the completion of the risk assessment, whichever is later. Moreover, § 7152(a)(5) provides guidance to businesses regarding the types of negative impacts they may consider.
RAs	339	Comment argues that the proposed regulations improperly extend privacy risk assessment obligations beyond the scope of the CCPA. Specifically, it criticizes requiring risk assessments for generative AI training, which it claims does not constitute ADMT and is therefore outside the CCPA's regulatory scope. Comment also argues that the regulation of deepfakes should be left to the legislature rather than the CPPA.	The Agency disagrees with this comment. The Agency has authority to require risk assessments for generative AI and deepfakes. The CCPA requires risk assessments to be conducted for processing activities that present significant risk to consumers' privacy, regardless of whether they render a significant decision about a consumer. This includes training uses of consumers' personal information. However, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at

			this time. The Agency also removed references to deepfakes to further simplify implementation at this time.
RAs	345	Comment states that the proposed regulations require businesses to assess and weigh data processing risks but lack concrete metrics for determining when privacy risks outweigh benefits. The concern is that businesses will be subjected to subjective and inconsistent regulatory decisions.	The Agency disagrees with this comment. The risk assessment requirements provide clear direction to businesses regarding how to conduct a risk assessment, including the necessary elements. The Agency disagrees with these requirements will lead to subjective or inconsistent regulatory decisions. The risks to consumers' privacy include guidance from the Agency about types of harms that businesses can consider and provides examples to help businesses identify them.
RAs	439	Comment expresses support for the transparency requirements in the proposed regulations, specifically §§ 7150 and 7152, which mandate that businesses disclose the underlying logic, assumptions, outputs, and the source, validity, and relevance of personal information used in ADMT. Comment emphasizes that clear, enforceable guidance will enhance protections and build consumer confidence.	The Agency agrees with this comment and notes comment's support.
RAs	605	Comment states that different entities in the AI value chain (e.g., developers vs. deployers) may not have access to the required information, making compliance difficult. For example, developers may not know how deployers will use their products.	The Agency disagrees with this comment. The risk assessment requirements clearly inform businesses regarding how to conduct a risk assessment, including the necessary elements. In addition, the requirements in §§ 7050 and 7153 regarding service providers, contractors, and businesses training ADMT for significant decisions ensures that businesses have all facts necessary to conduct a risk assessment.
RAs	606, 1197, 1226	Comment claims that the excessive details and documentation required in risk assessments drive up compliance costs that may be passed to consumers,	The Agency disagrees with this comment. The regulations appropriately balance protections for consumers and the burden on businesses to submit the

		force companies to hire experts and lawyers, and dedicate significant resources away from normal business operations and risk mitigation. The Agency's claim that assessments are cost-effective is unsupported, relying on GDPR-related data rather than evidence specific to these regulations.	required information. Businesses also can leverage their existing compliance processes to comply with the requirements in § 7152. Businesses may consult with external stakeholders but are not required to do so. These regulations encourage cost-effective compliance. Businesses can use the clearly stated requirements in the regulations and their existing compliance processes to conduct the risk assessments.
RAs	808	Comment requests that examples of compliant versus non-compliant risk assessments be made available so that companies have an opportunity to anticipate the requirements of the assessments.	The Agency disagrees with this comment. The regulations clearly identify the risk assessment requirements, both in conducting the risk assessment and submitting it to the Agency. The Agency also already provides several examples for specific requirements in the regulations and does not believe examples of full risk assessments are necessary at this time.
RAs	842	Comment suggests that audits ought to be independent and conducted by expert, "at-risk" third parties. Additionally, unless there are an objective set of rules, such as a government-approved certification scheme (e.g., Article 42 of the GDPR), audits will not be uniform and thus will be rendered largely ineffective.	The Agency disagrees with this comment. Businesses must conduct risk assessments, and may involve external stakeholders, such as independent experts, as necessary. Mandating the involvement of external stakeholders is not necessary at this time. With respect to a certification scheme, this is not necessary. § 7152 already provides clear rules regarding how to conduct a risk assessment.
RAs	1002	Comment asserts that the proposed regulations require regular risk assessments for AI used in significant healthcare decisions, but FDA regulations already mandate rigorous safety and effectiveness procedures under its Quality System Regulation (QSR).	The Agency disagrees with this comment, to the extent that it argues that businesses do not need to a conduct a risk assessment. The CCPA requires that businesses conduct a risk assessment for processing that presents significant risk to consumers' privacy. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. In addition, to the extent a business already has conducted a risk assessment to comply with FDA regulations, it may leverage its

			existing compliance processes to meet the requirements in § 7152.
RAs	1072	Comment recommends strengthening the required elements of risk assessments to ensure a comprehensive evaluation of potential harms and biases in ADMT usage.	The Agency disagrees with this comment. The risk assessment regulations ensure that businesses identify risks to consumers for various processing activities, including the use of ADMT for a significant decision. They also provide guidance about different privacy risks to consumers, such as unlawful discrimination, and potential safeguards, such as policies to address harms from lack of accuracy and unlawful discrimination. The regulations provide both clarity and flexibility to businesses conducting risk assessments, and additional requirements are not necessary at this time to address harms and biases from ADMT usage.
RAs	1239	Comment suggests that constant updates and notifications may create a false sense of security as these assessments do not always capture the dynamic and evolving nature of security threats. Rigidly applying this requirement to every use of ADMT, whether or not it is meaningful for the consumer, could lead to an excessive focus on process documentation rather than on the real-time monitoring and active management of security threats. Comment believes that allowing flexibility in meeting transparency, risk assessment, and data quality requirements would better balance innovation with security.	The Agency disagrees with this comment. The update requirements are necessary to ensure that risk assessments remain accurate, particularly after a material change to the processing. This is consistent with both Colorado's and GDPR's approach. The Agency has also revised the risk assessment requirements to further simplify implementation for businesses at this time.
RAs	1272	Unlike audits, comment argues that risk assessments should evaluate how well an organization's security measures address cyber threats in a flexible, context-dependent manner.	The Agency agrees in part with this comment, to the extent that it supports risk assessments as a tool to protect consumers' personal information. Additionally, the regulations provide guidance about different

			privacy harms and safeguards that businesses may consider, which provides both clarity and flexibility.
RAs	1273	Comment suggests that risk assessments should remain internal, often conducted under client privilege. Requiring submission to the Agency could discourage organizations from fully investigating vulnerabilities for fear of regulatory consequences.	The Agency disagrees with this comment. The CCPA requires submission of risk assessments to the Agency. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. In addition, the risk assessments do not require attorney-client privileged information to be included in the risk assessment. Further, the risk assessment requirements provide clear guidance to businesses about how to appropriately conduct a risk assessment with relevant stakeholders.
RAs	1274	Comment advocates that the risk assessment section should align with the ADMT section by exempting security, fraud prevention, and safety-related data processing from assessment requirements.	The Agency disagrees with this comment. The security, fraud prevention, and safety exemption in ADMT disclosures helps protect both businesses and consumers against external bad actors. Risk assessments are internal-facing tools, and risk assessment reports are submitted to the Agency and Attorney General, so there is no need to provide a similar exemption to protect against external bad actors.
RAs	1278	Comment proposes that the Agency allow businesses to demonstrate compliance with existing privacy risk assessment laws, such as GDPR's Article 35 and the Colorado Privacy Act, to satisfy the proposed requirements. The current proposal mandates risk assessments for any use of personal information deemed to present "significant risk to consumers' privacy," which duplicates obligations already imposed by other regulations. Instead of requiring redundant compliance efforts, the Agency should focus on promoting clear security benchmarks, fostering a skilled cybersecurity workforce, and encouraging	The Agency disagrees with this comment. The regulations explicitly allow businesses that comply with other laws to use their existing risk assessments to comply with § 7152. The regulations have been revised to provide an example of how a business may do so. This enables businesses to leverage existing compliance processes to comply with § 7152. In addition, the CCPA requires the Agency to issue regulations regarding risk assessments for processing that presents significant risk to consumers' privacy. The Agency cannot amend

		industry-wide information sharing to enhance data protection.	the CCPA or adopt regulations inconsistent with the CCPA.
RAs	1525	Comment argues that § 7152 should only apply to ADMTs trained on personal information, which many testing tools are not. It recommends case-by-case agency requests for risk assessments rather than automatic submissions and insists that non-AI, non-personal-data uses should be exempt. Lastly, comment argues that the Agency should recognize that testing/assessment organizations use risk assessment controls to identify risks, and that risk management/assessment includes certain threat, vulnerability, and other analyses. Comment recommends adding two requirements regarding business's development, implementation, and maintenance of a vulnerability and threat management program, and regular performance of a vulnerability and threat assessment.	The Agency disagrees with this comment. § 7152 applies to the processing activities set forth in § 7150(b), and the definition of ADMT already requires the processing of personal information. Additionally, the CCPA requires submission of risk assessments to Agency, which cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Moreover, testing/assessment organizations may leverage existing compliance processes to conduct a risk assessment under the CCPA. With respect to comment's recommendations regarding threats and vulnerabilities, the CCPA and other laws already require that businesses have reasonable security; however, the risk assessment requirements do not prohibit a business from implementing comment's recommendations as part of their safeguards for a processing activity.
RAs	1584	Comment suggests that the regulations acknowledge that the identification of risk and harm is largely a context-specific exercise.	The Agency disagrees with this comment, to the extent that it suggests that the regulations are not adaptable to a variety of contexts. The regulations balance providing protections for consumer privacy with flexibility for businesses to come into compliance. They are adaptable to a variety of situations and businesses while providing clarity regarding how to conduct a risk assessment.
RAs	1585	Comment urges the Agency to ensure that regulatory classifications of significant/high-risk or low-risk be rebuttable through risk assessments and demonstrable organizational methods and mitigations.	The Agency disagrees with this comment. It is unclear how comment's recommendation would work. Regardless, a rebuttable presumption is unnecessary. The CCPA is clear about the goal of a risk assessment, which is reflected in § 7154.

RAs	1586	Comment asks the Agency to provide businesses with a template to guide preparation of abridged risk assessments and enable submission through the Agency's website.	The Agency disagrees with this comment. The regulations are clear about what a business must include in submissions to the Agency. Additionally, the Agency has revised the regulations and removed the requirement regarding abridged risk assessments to simplify implementation for businesses at this time.
RAs	1587	Comments asks the Agency to engage with data protection agencies and regulators outside of California to establish interoperable risk assessment frameworks and templates with guidance to bridge legal and technical differences between legal systems.	The Agency agrees in part with this comment, to the extent it supports interoperability. The Agency disagrees in part with this comment, to the extent it suggests that the regulations do not enable businesses to bridge differences across jurisdictions. The requirements are consistent with approaches taken in other jurisdictions, such as those in the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about their obligations. Businesses can also leverage existing compliance processes to comply with § 7152.
RAs	1374	The threshold activities that require risk assessments far exceed those required by other U.S. privacy statutes and do not focus on the processing of PI in a manner that presents a significant risk to consumers' privacy as required by statute. The CPPA should harmonize risk assessment thresholds to those activities where there is settled consensus that such assessments should be performed: (1) the sale of PI, (2) the sharing of PI for targeted advertising, (3) the processing of large amounts of sensitive personal information (i.e., 1 million or more consumers or households), and (4) significant decisions that pose significant privacy risks. The regulations should incorporate a threshold volume of SPI processing that triggers requirements as the CCPA definition of SPI is	The Agency disagrees with this comment. The risk assessment requirements are consistent with approaches taken in other jurisdictions, including those in the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses regarding what is in scope. In addition, comment's proposed thresholds are not consistent with those frameworks, which do not use a sensitive personal information volume threshold, limit the threshold regarding processing sensitive personal information to 1 million or more consumers, or use the standard of "significant decisions that pose significant privacy risks." Those jurisdictions also contain thresholds beyond the comment's proposed language. Further, comment's proposed language is less effective than the regulations at protecting consumer privacy, because it would not

		broader than other US privacy frameworks (e.g., includes account credentials).	require risk assessments for other processing activities that pose significant risk to consumers' privacy, such as certain automated processing or training uses of consumers' personal information.
RAs	258	Comment argues that the regulations in §§ 7152(a)(6)(B), 7153(a)-(b), and 7156(b) are unclear as to which responsibilities lie with the vendor (the provider or developer) and which lie with the user of the ADMT (the employing entity).	The Agency disagrees with this comment. The regulations are clear in Article 10 and § 7050 about the requirements for businesses, service providers, and contractors.
RAs	1913	The risk assessment scope is too broad because it uses the definitions of ADMT and AI. The definition of AI is all software because all software "generates outputs that can influence physical or virtual environments" and ADMT includes AI and everything that "substantially facilitates human decisionmaking," with the only limiting factor being whether the technology was a "key factor" in human decisionmaking. This can include email and texts, booking software, listing notifications, and application tracking.	The Agency disagrees with this comment. The Agency has revised the definition of 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 simplifying implementation for businesses at this time. With respect to AI, the Agency deleted the definition of artificial intelligence as unnecessary and removed references to AI throughout the regulations to further simplify implementation for businesses at this time.
RAs	1688 1689	Risk assessment requirements are consistent with existing laws and the Agency's mission. Risk assessments submitted to the Agency fall squarely within CA's constructional right of access, as well as the right of access under the CA Public Records Act. Risk assessments relate to the public's business because they directly impact both the public's individual rights under the CCPA and the CCPA's obligations thereunder, and any risk assessment information disclosed to the Agency is "used[] or retained" under the meaning of the Public Records	The Agency agrees in part with this comment, to the extent it supports the regulations. However, the Agency cannot amend the Public Records Act ("PRA") or adopt regulations inconsistent with the PRA. Additionally, providing disclosures to the Agency does not equate to it being exposed; whether information in the Agency's records is subject to public disclosure depends on the specific information and whether an exception to the PRA applies.

		Act. Risk assessment transparency aligns with the California Uniform Trade Secrets Act. CCPA risk assessments are neither "trade secrets" nor are they acquired or disclosed through "improper means" such that it would qualify for protection. They are completed for the purpose of regulatory compliance and disclosure, not for economic value. Also, much of the information required in a risk assessment is already intended or required to be made public under the CCPA. The only categories that are unique are the method and technology used for data collection and the benefit-impact analysis, and neither raise CUTSA concerns.	
RAs	1690, 1692, 1972, 1974	Public transparency of risk assessments is in the Agency's best interests. Public transparency can improve enforcement and better protect the public by allowing the public to review them and submit tips to the Agency for businesses or trends to investigate. Making risk assessment information public by default can effectively reduce the costs of fielding Public Records Act requests or lawsuits seeking access to the information. It can also help business improve their own risk assessment and data collection practices. The information contained in the abridged risk assessments should be made available in a machine readable, searchable database available on the Agency website. The public database will help to protect consumers by allowing civil society organization and community groups to analyze the assessments and push for more privacy-protective business practices based on their contents. The Agency and Attorney General face resource constraints, making timely identification of issues difficult and public disclosure could help to alleviate	The Agency disagrees with this comment. The CCPA requires submission of risk assessments to the Agency. The Agency cannot amend the CCPA or Public Records Act or adopt regulations inconsistent with either law. Further, the Agency will provide a public report summarizing the risk assessments filed with the Agency, consistent with the requirements of the CCPA. (Civ. Code § 1798.199.40(d).)

		this problem. Public access mirrors public stakeholder engagement expectations in leading AI risk management frameworks. With public disclosure and transparency, businesses will be incentivized to implement more rights-protective business practices, explain publicly what negative impacts their practices cause, and identify what safeguards they will adopt to mitigate those impacts.	
RAs	1693, 1975	The Agency should have explicit authority to review and deny a business's certification that the benefits of its processing activities outweigh the negative impacts of that processing. There must be an effective oversight mechanism to ensure that the benefits and risks are appropriately and accurately assessed, and the Agency is the best suited entity to oversee this. The Agency should include in the regulations an explicit mechanism for the Agency to question and take action against deficient risk assessments.	The Agency disagrees with this comment, to the extent it implies that the Agency does not already have authority to act on violations of the risk assessment requirements. As with other violations of the CCPA, the Agency has enforcement authority if a business is not complying with the law.
RAs	1745	Comment generally supports the risk assessment requirements and believes risk assessments are valuable for encouraging early consideration of data processing dangers.	The Agency agrees with this comment and notes comment's support.
RAs	1790, 1791, 1792, 1793, 1794, 1795	Comment supports Article 10's introduction of mandatory risk assessments for AI, ADMT, and high-risk data practices but criticizes that the regulation does not sufficiently account for the expanding attack surface introduced by IoT, unmanaged assets, and modern AI supply chains. Comment believes that adopting continuous security validation, automated asset discovery, and real-time exposure management as part of their compliance efforts is crucial. Comment points out that the regulation should explicitly address AI supply chain security risks, particularly in	The Agency disagrees with this comment. The risk assessment requirements provide clear direction about how to conduct a risk assessment and are adaptable to a variety of use cases and industries. The regulations already provide guidance to businesses regarding risks to consumers' privacy and potential safeguards for consideration. This guidance is nonexhaustive, and businesses may consider other risks and safeguards, including those recommended by comment, when conducting a risk assessment. In addition, to the extent businesses are using existing frameworks, such as

		cases where businesses rely on third-party AI models, cloud-based AI services, or externally trained datasets. Businesses conducting risk assessments under CPPA should be required to document AI supply chain dependencies, implement Software Bill of Materials for AI models, and establish contractual safeguards ensuring AI service providers adhere to CPPA-compliant privacy and security practices. Comment urges the Agency to require real-time risk monitoring and automated compliance validation. Businesses subject to Article 10's ADMT risk assessment requirements should deploy AI-driven anomaly detection systems that identify data drift, adversarial model tampering, and unauthorized access to AI-powered IoT systems. Additionally, implementing cryptographic attestation mechanisms to verify the authenticity of AI models and IoT firmware will ensure that AI-driven authentication and decision-making systems cannot be manipulated through adversarial attacks. Comment suggests that the proposed regulations should consider quantum security readiness. The absence of post-quantum cryptographic (PQC) transition requirements leaves businesses exposed to long-term cryptographic vulnerabilities, particularly those handling consumer financial data, biometric authentication systems, and AI-powered security applications. Comment recommends implementing hybrid cryptographic models and require cryptographic attestation mechanisms for AI models used insecurity-critical applications. Comment suggests that the Agency should address that AI model deployment in multi-cloud and hybrid environments increases exposure to misconfiguration, IAM flaws, and supply chain threats.	those recommended by NIST, they may leverage those compliance processes to meet the requirements in 7152. Additional regulations are not necessary at this time.

		The regulation should expand its guidance on cloud security, enforce zero-trust frameworks, and align with NIST SP 800-207. Comment argues that while Article 10 is a necessary step in advancing AI security and consumer protection, it is incomplete without explicit attack surface management, AI supply chain security, IoT risk mitigation, and post-quantum cryptographic safeguards. Comment strongly urges strengthening Article 10 by mandating continuous attack surface management for AI and IoT ecosystems, requiring cryptographic attestation for AI-driven authentication and biometric verification systems, enforcing cloud security, and incorporating AI supply chain risk management into the risk assessment framework.	
RAs	1820, 1821	Comment recommends developing public-facing supplementary resources that includes a reporting structure that prompts and guides the assessor on the steps that need to be carried out (and the correct order) when executing the risk assessment. As an example, NIST follows this structure as part of the Cybersecurity Framework 2.0 publication. Comment recommends a publication that quantifies risks that risk assessors can reference and compare with the business's risk assessment output. This allows businesses to leverage analysis performed once that all businesses can compare against and eliminate the opportunity for duplicative work across cybersecurity auditors.	The Agency disagrees with this comment. The regulation is reasonably clear based on the plain meaning of the word(s) and specifically identifies the requirements. In addition, the Agency has revised the regulations to provide additional clarity about how businesses must conduct a risk assessment. The Agency believes that no further clarification is needed at this time.
RAs	1971	Risk assessments are crucial for businesses to assess how privacy invasive their practices are and for consumers to understand the risks associated with	The Agency agrees with this comment and notes comment's support.

		the processing of their personal information. The regulations are a strong start.	
RAs	1351, 1377, 1378	Comment argues that the regulations take a one-size-fits-all approach by requiring a number of granular topics to be addressed, regardless of the processing activity, whether those elements are relevant, or even if the topic has a relationship to the Agency's authority as a privacy regulator. For example, every risk assessment must include the retention period for personal information and the criteria used to determine the retention period, as well as the technology used for the processing. The regulations also suggest that risk assessments should consider, for example, "economic harms" that ADMT may cause, such as higher prices or lower wages, which are unrelated to the Agency's mandate as a privacy regulator. Consequently, the regulations depart from the purposes of risk assessments – to identify and address identified significant privacy risks – in favor of a paperwork exercise, which diverts resources that will not benefit consumers. The Agency should revise the regulations to permit businesses the flexibility to determine and address those topics that are relevant for the processing activity in completing risk assessments. This would promote interoperability with other privacy frameworks (e.g., Colorado). Comment also argues that mandating granular assessment is inappropriate and transforms the risk assessment into a GDPR-like privacy impact assessment. The regulations should not prohibit the processing activity if the risks to consumers outweigh the benefits and thus suggest that the assessment must be concluded before the processing activity begins. Privacy impact assessments are typically exercises with respect to a	The Agency disagrees with this comment. Each of the requirements are necessary to ensure the risk assessments are meaningfully conducted and not a paperwork exercise. The examples illustrate this point. Specifically, the retention period for personal information is a key element to identify potential risks to consumers' privacy, such as unauthorized access to information that is retained longer than necessary. Similarly, consumers can face economic harms as a result of processing of their personal information, and these are privacy harms. Moreover, § 7154 has been revised to further clarify the goal of a risk assessment as stated in the CCPA, which the Agency cannot amend. The also regulations harmonize with other frameworks, such as GDPR and the Colorado Privacy Act, while furthering the intent and purposes of the CCPA, and clearly inform businesses about their obligations. Further, § 7156 enables businesses to leverage their risk assessments completed for other purposes, provided they contain all of the information required by California or are supplemented to include any missing information. The regulations also explicitly require that the risk assessment is conducted before initiating the processing activity, with updates for accuracy or to address material changes. (§ 7155.) Risk assessments are conducted for specific processing that presents significant risk to consumers' privacy, as set forth in the CCPA. It is also unclear what comment means by "processing at a category level" but the CCPA is clear about what a risk assessment must cover, and the regulations cannot amend the statute. Comment also has not identified what beneficial "compliance

		particular project or product, whereas a risk assessment is intended to cover overall processing at a category level.	functions" resources will be diverted away from, nor has it provided evidence of this issue. Nonetheless, the Agency does not believe this is the case. Risk assessments provide benefits to both businesses and consumers, by ensuring that businesses are identifying risks to their privacy and managing those risks prior to processing consumers' personal information.
RAs	777	Comment suggests expanding § 7152(a)(6)(B) to require businesses to disclose how they mitigate all risks, not just discrimination, and to clarify the extent to which these safeguards eliminate or reduce risks. Comment also suggests that the final regulations should clarify that businesses must comply with § 7152(a)(6)(B)(i)-(ii), even when obtaining ADMTs from another party, and that § 7152(a)(6)(B)(iii) imposes additional requirements. Additionally, businesses supplying ADMTs must provide comprehensive risk assessment details to ensure transparency. § 7153 should mandate that businesses share their own risk assessments with recipient parties to facilitate informed evaluations.	The Agency disagrees with this comment. The Agency has revised § 7152(a)(6)(B) so it is no longer mandatory, and revised § 7152(a)(6) overall to clarify that businesses must identify what safeguards they plan to implement. In addition, because the regulations are intended to apply to variety of industries and contexts, § 7156(a)(6) provides a nonexhaustive list of safeguards that a business may consider. Businesses may consider other safeguards and consider how these safeguards eliminate or reduce risks. This approach simplifies implementation for businesses at this time and provides them with flexibility to come into compliance. Additionally, the suggested language is not necessary. A business subject to § 7153 must provide all facts necessary for a recipient-business to conduct their risk assessment. The business may choose how it provides these facts, such as sharing their own risk assessments or otherwise finding other methods to provide the necessary facts.
RAs	1171, 1602	Comment claims that §§ 7050(h) and 7153(a) impose overly broad obligations on service providers by requiring them to provide "all facts" needed for assessments. The rules should instead require them to provide necessary information relevant to their role in the AI process. Comment also cautions that the current drafting may lead to unclear responsibilities.	The Agency disagrees with this comment. The requirements are not overly broad. § 7050(h) is clear that a service provider is only required to disclose facts necessary for the business to a conduct the risk assessment that are within the service provider's possession, custody, or control, and only with respect to personal information the service provider collected

		Both provisions should be revised. Comment recommends aligning this expectation with the GDPR, which bases assistance on the nature of processing and available information.	pursuant to its written contract with the business. Similarly, § 7153(a) only requires a business that makes ADMT available to other businesses to make a significant decision to provide all facts available to the business that are necessary for the recipient-business to conduct its own risk assessment. These requirements are appropriately limited to facts that are necessary to conduct a risk assessment and that are within the possession, custody, or control of or available to the disclosing entity.
RAs	1451	Comment suggests deleting requirements for ADMT in risk assessments in §§ 7152(a)(6) and 7153.	The Agency disagrees with this comment. However, to simplify implementation at this time: (1) the mandatory safeguards in § 7152(a)(6) are now provided as guidance for businesses to consider in their risk assessments; (2) § 7153(b) has been deleted; and (3) § 7153(a) has been revised to focus on businesses making ADMT available to others to make a significant decision.
RAs	164	Comment suggests that the proposed risk assessment requirements should be harmonized with existing federal and international frameworks (e.g., GDPR) to avoid redundant compliance burdens. The draft rules set a lower threshold for conducting risk assessments than comparable frameworks, forcing businesses to generate excessive reports on routine activities instead of focusing on genuinely high-risk scenarios. Additionally, requiring retroactive assessments and immediate updates for minor changes is unrealistic and resource intensive.	The Agency disagrees with this comment. Each of the thresholds in § 7150(b) present a significant risk to consumers' privacy. In addition, the risk assessment regulations are consistent with other risk assessment frameworks, such as those in the EU and Colorado. The regulations require a risk assessment for processing that presents a significant risk to consumers' privacy that occurs or continues after the effective date of these regulations. They also require updates every three years or when there is a material change, which balances protections for consumer privacy with providing flexibility for businesses in meeting their compliance obligations. The regulations have also been revised to give businesses up to 45 days to update their risk assessments when there is a material change.

RAs	1629	Comment argues that § 7157(a), which requires annual submission of risk assessments, conflicts with § 7155(a)(2), which requires updates every three years. This annual submission requirement is burdensome and costly, potentially deterring innovation.	The Agency disagrees with this comment. § 7155 and § 7157 do not conflict and are clear about a business's obligations. A business must review, and update as necessary, their risk assessment every three years. A business must also annually submit certain risk assessment information to the Agency. Further, the regulations balance protecting consumers' privacy with providing flexibility for businesses to come into compliance. Further, respecting consumer privacy and data protection is not contrary to innovation and entrepreneurship; rather, the regulations foster the development of privacy-by-design products and services. Nevertheless, the Agency has modified the regulations to significantly reduce costs.
RAs	604, 871	Comment highlights that requiring businesses to compile all the information in § 7152 before processing even begins makes compliance unworkable, as many details will be unknown at that stage. Comment suggests that risk assessments should not impede updating processing activities. While the regulations provide 24-months to complete a risk assessment on processing that took place prior to the effective date, the language indicates that no new processing activity can take place until a risk assessment is done.	The Agency disagrees with this comment. A risk assessment is necessary before the business conducts the processing because otherwise the processing activity could have negative impacts on consumers' privacy that a business would not identify and mitigate until after it started the activity. In addition, a business can always update the risk assessment after more information is known to it.
RAs	778	Comment suggests that businesses should be required to document stakeholder consultations on bias detection and risk mitigation in ADMTs. If consultations were not conducted, businesses must explain why. Additionally, § 7152(a)(6)(A) should mandate — rather than suggest — that businesses assess the need for human oversight in ADMT use. Businesses should evaluate whether trained	The Agency disagrees with this comment. Comment's recommendations are not necessary at this time. With respect to § 7151(b), whether and how the business consults with external stakeholders to conduct the risk assessment is within the business's discretion. The risk assessment must still be accurate and meet the requirements set forth in § 7152. With respect to § 7156(a)(6), the safeguards identified are listed as

		personnel can review and override ADMT outputs to prevent harmful automated decisions.	guidance for businesses to consider when identifying potential safeguards in their risk assessment. This regulation has been revised to correspond to the revised definition of ADMT and to provide flexibility for businesses to come into compliance.
RAs	1124	Comment argues that the regulations, particularly §§ 7151 and 7152, impose vague and overly broad risk assessment requirements, leading to excessive compliance burdens. The requirement to include many "relevant individuals" and potentially external parties in risk assessments could result in inefficiency and delays.	The Agency disagrees with this comment. The regulations provide clear guidance about what is in scope and are not overly broad. The Agency has revised the regulations to further clarify the responsibilities of a business's employees in § 7151(a), and to simplify implementation for businesses at this time. Additionally, involving external parties can enable efficiencies in the risk assessment process, and § 7151(b) provides clarity that a business may involve external parties but does not require their involvement.
RAs	2056	Comment argues companies should be required to mitigate all predictable privacy risks even where specific impacts were not anticipated.	The Agency disagrees with this comment. A business must identify relevant risks and safeguards in its risk assessments. The Agency does not believe that comment's recommendation is necessary at this time.
RAs	1132, 1154, 1547	Comment urges the Agency to revise the regulations to differentiate between first-party and third-party data processing, remove the new definition of "behavioral advertising," and remove "behavioral advertising" from the definition of "extensive profiling" in § 7150 (b)(3)(B)(iii). Comment states that behavioral advertising should not be included as a category of "extensive profiling" because advertisements are incapable of making decisions; rather, advertisements are a method of communication used to promote products and services. This threshold would extend to all behavioral ads rather than only CCBA (the focus of the statute) and impose detailed requirements that are not calibrated to the potential risk, since no	The Agency disagrees with this comment. The regulations are consistent with the CCPA and further its intent and purposes. (*See* Civ. Code § 1798.185(a)(14)-(15).) Nevertheless, the regulations have been revised to remove the profiling for behavioral advertising threshold, to simplify implementation for businesses at this time.

		consumer data is being shared with third parties or combined with other third-party data. Comment suggests striking § 7150(b)(3)(B), or at minimum, subpart (iii).	

ARTICLE 11. AUTOMATED DECISIONMAKING TECHNOLOGY

Section of Regulation	Comment Numbers	Summary of Comments 45-Day Comment Period	Agency Response
7200	184	Comment suggests the addition of §§ 7200(b) or (c): "Businesses shall not be required to audit individual employees' activities for whether they are using ADMT for the purposes listed in § 7200(a)."	The Agency disagrees with this comment. The regulations' requirements are reasonably clear, and they provide flexibility for businesses regarding how they ensure their compliance. The Agency believes that no further clarification is needed at this time.
7200	191, 683, 1386, 1401	Comment asserts that the ADMT requirements should provide businesses with 24 months to come into compliance. This approach would align with other new provisions and with other U.S. state privacy statutes. Such timing also creates consistency with the 24-month implementation period for cybersecurity audits and risk assessments. In addition, businesses should also be given 24 months to come into compliance with modifications to the existing regulations.	The Agency disagrees with this comment. However, the Agency has added § 7200(b) to provide a specific date, January 1, 2027, by which a business must be in compliance with the requirements in Article 11. This revision gives businesses additional time to implement the regulations. With respect to the updated regulations, the Agency does not believe additional time to come into compliance is necessary at this time.
7200	711	Policymakers around the country are already developing regulations and guidance that would govern the insurance industry's use of ADMT. Insurance companies already comply with extensive laws on ADMT and anti-discrimination, including requirements from the California Department of Insurance, NYDFS, and NAIC's AI Model Bulletin. The Agency should avoid additional requirements that would create potentially	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency modified the definition of 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 simplifying implementation for businesses at this time.

		conflicting requirements and more regulatory uncertainty.	Separately, the Agency revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. Further, the CCPA makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal or state law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196.)
7200	824	Comment suggests that all personal information used in any manner to reach a decision with meaningful impact to the consumer be available for validation, including dispute and/or correction.	The Agency disagrees with this comment, to the extent it suggests that the regulations do not provide consumers with information about how certain decisions were made with respect to them. With respect to the regulations, § 7222 addresses the information that businesses must provide in response to consumers' requests to access ADMT. With respect to personal information, consumers also have a right to know and a right to correct under the CCPA, and existing regulations address how businesses must handle consumers' requests to know and requests to correct (*see* §§ 7023, 7024), so comment's recommendation is not necessary. Further, the Agency has revised the regulations to focus on the use of ADMT to make a significant decision to further simplify implementation for businesses at this time.
7200	825, 826	Comment recommends that social behavior/social scoring, which is a form of personal information, is prohibited from usage in accordance with federal law that protects speech or similar prohibitions such as by fair housing, and fair credit law. Additionally, such prohibitions are afforded under Article 5 of the EU AI Act, unless deemed relevant and having occurred during a "'certain period of time' - reasonably applicable."	Comment does not appear to be on the proposed action.

7200	998	Comment recommends explicitly linking ADMT to definitions of "significant decision" and "extensive profiling" in § 7200.	The Agency disagrees with the comment. The Agency has revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time.
7200	1291, 1173	Comment argues that the current definition of "significant decision" includes "access to" employment opportunities, which is too broad. This could unintentionally include tools with minimal privacy or discrimination risks, such as automated interview schedulers or security programs preventing bots from accessing job boards. Comment recommends refining the definition to focus only on decisions that provide or deny a service, benefit, or opportunity. Comment recommends replacing "access to" with "selection for" employment to focus regulatory scrutiny on automated systems that directly impact hiring or employment outcomes. This would enhance consumer protections without overburdening low-risk technologies.	The Agency disagrees with the comment. The term "access to" is not overly broad. However, the Agency revised the definition of significant decision, including removing the phrase "access to."
7200	1309, 1607	Comment asserts that the regulations impose ADMT requirements on activities that do not involve direct decision-making, such as training models and behavioral advertising. Comment recommends limiting ADMT obligations to decisions that materially affect consumers' legal or financial rights, such as access to housing, employment, or healthcare. § 7200 creates time- and resource-intensive requirements on businesses engaged in common and low-risk processing activities, which would also overburden the enforcement efforts of the Agency. Comment suggests that the regulations should primarily cover uses of ADMT that are solely automated and produce legal or similarly significant effects. Comment suggests	The Agency disagrees with the comment, to the extent it suggests that the regulations would be overly burdensome. Nevertheless, the Agency modified the definition of ADMT to focus on a higher-risk use of ADMT, which is a use without any human involvement. This balances protections for consumer privacy and simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. This includes removing the behavioral advertising thresholds from the regulations and removing the training ADMT threshold from Article 11. The Agency has made efforts to limit

		excluding training models and behavioral advertising from these requirements.	the burden of the regulations while implementing the CCPA.
7200	1936	The Agency should delete the reference to ADMT and replace with "engages in any of the following activities… profiling in furtherance of decisions that produce a significant decision concerning a consumer." Comment notes that the definition of "profiling" already encompasses ADM.	The Agency disagrees with this comment. The CCPA makes clear that ADMT includes profiling and directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The regulations must address businesses' uses of ADMT to align with the CCPA's direction to the Agency. The Agency modified the definition of ADMT to focus on a higher-risk use of ADMT, which is a use without any human involvement. This balances protections for consumer privacy and simplifying implementation for businesses at this time. Separately, the Agency revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time.
7200	1138	Comment argues that the regulations fail to provide a workable solution for situations where only part of the data used in an ADMT-based decision is subject to a CCPA exemption. It is unclear whether the entire decision is exempted or if only certain data is excluded. This ambiguity creates compliance challenges for insurers.	The Agency disagrees with this comment. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; the CCPA's exemptions apply to the regulations. However, if an exemption does not apply and a business is using ADMT for a significant decision, it must comply with Article 11's requirements for that use. The regulations are clear and do not create compliance challenges.
Previous 7200(a)(3), 7221(b)(2)(B)	714	Comment recommends that the Agency clarify whether businesses must verify a consumer's request to appeal ADMT under § 7221(b)(2)(B). Comment also suggests changing the language in § 7200(a)(3) from "is capable" to "is being used" to preserve distinctions related to high-risk uses of ADMT.	The Agency disagrees with this comment. With respect to verification, the regulations are clear that a business must comply with the verification requirements in Article 5 when responding to a request to appeal. With respect to the language in § 7200(a)(3), comment's suggestion is not necessary

			because the Agency has removed the training ADMT threshold from Article 11.
7200(a)	171	Comment suggests revision as follows: "A business that uses automated decisionmaking technology in any of the following ways must comply with the requirements of this Article, provided that this Article shall not apply to use of automated decisionmaking technology in contexts in which data collected would be subject to the exceptions set forth in Civil Code Sections 1798.145, subdivisions (c)-(g), or 1798.146, subdivisions (a)(1), (4), and (5)[.] "	The Agency disagrees with this comment. However, the Agency has revised § 7200 to focus on the use of ADMT for significant decisions and revised the definition of ADMT to address the higher-risk use of ADMT without any human involvement. The Agency has 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 cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
7200(a)	179	Comment suggests the revision of § 7200(a): "A business that uses automated decisionmaking technology in any of the following ways must comply with the requirements of this Article except as set forth in subsection (b) below[.]" In addition, a new § 7200(b) would be added as follows: "Automated decisionmaking technologies that are subject to examination or supervision by a federal prudential regulator are not subject to the requirements of this Article."	The Agency disagrees with this comment. The CCPA applies to "businesses" and does not exempt financial institutions. (*See* Civ. Code §§ 1798.140(d), 1798.145(e).) The CCPA also makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196.) Further, the CCPA includes data-level exemptions for (1) information subject to the Gramm-Leach-Bliley Act and implementing regulations or the California Financial Information Privacy Act and (2) the processing of personal information by certain entities, as long as the activity is regulated by the FCRA, and the processing is as authorized by the FCRA. (*See* Civ. Code §§ 1798.145(d), (e), 1798.196.) The CCPA directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA

			or adopt regulations inconsistent with the CCPA. Although the Agency strives for alignment with other laws, the Agency must comply with California law and use its discretion to adopt requirements appropriate to California. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA.
7200(a)	183	Comment suggests that the following revision should be made to definitively ensure that the rules do not create any ambiguity that they apply to automation in relation to business customers, as opposed to consumers: "A business that uses automated decisionmaking technology to make decisions about natural persons who are California residents in any of the following ways must comply with the requirements of this Article[.]"	The Agency disagrees with this comment. The CCPA and the regulations are clear about when a business's use of ADMT will be subject to the regulatory requirements.
7200(a)	982	Comment suggests that the definition of "significant decision" should be streamlined into § 7001 to avoid redundancy across multiple sections.	The Agency agrees with this comment and has moved the definition into § 7001(ddd). The Agency has also revised the definition of significant decision to provide additional clarity and guidance for businesses, and to further simplify implementation for businesses at this time.
7200(a)	1101, 1205, 1595, 1624, 1661, 1847	Comment argues that the Agency's proposed regulations on ADMT and its introduction of "extensive profiling" exceed the statutory mandate under the CCPA and creates unnecessary burdens. Instead of regulating only the use of ADMT, the rule extends to technologies capable of being used for decisionmaking, which goes beyond the intended scope. It should be removed because it overextends the Agency's role, especially by including low-risk activities like behavioral advertising, personalization using first-party data, and "public profiling," which may also conflict with the CCPA's exclusion of publicly available information. In	The Agency disagrees with this comment. The ADMT and risk assessment regulations are within the Agency's authority and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(14), (15).) However, the Agency has revised the regulations to focus on the use of ADMT for significant decisions and revised the definition of ADMT to address the higher-risk use of ADMT without any human involvement. The Agency has also revised the regulations to remove the profiling for behavioral advertising threshold, to simplify implementation for businesses at this time.

		addition, the CCPA only provides a right to opt-out of sharing personal information, not targeted advertising within a business's own services. First-party advertising allows businesses to customize offerings and make their services more useful to consumers — and, in the case of app-based platforms, continue to offer more efficient and value-accretive support for local business partners.	
7200(a)	1458	Comment recommends changing the definition of "significant decision" for when the regulations apply to the use of ADMT. Comment proposes deleting language related to access, allocation or assignment of work, certain compensation, extensive profiling, and training of ADMT. Comment also proposes adding language regarding statutory exemptions and the phrase "in emergency situations" within the definition of "essential goods and services." Comment also proposes changing "includes" to "means."	The Agency disagrees with this comment. However, the Agency revised the definition of "significant decision" to provide additional clarity for businesses, and to further simplify implementation for businesses at this time. This includes deleting the phrases "access to" and "essential goods or services," and changing the word "includes" to "means." The Agency also deleted the extensive profiling and training ADMT thresholds and has revised § 7200 to focus on the use of ADMT for significant decisions to simplify implementation at this time. With respect to compensation decisions, the CCPA explicitly provides privacy protections to employees and independent contractors, and provides consumers with rights to access and opt-out of ADMT. The Agency has determined that a business's use of ADMT for these types of decisions presents significant risk to consumers' privacy and has accordingly retained it in the revised definition of "significant decision." The Agency has similarly retained "allocation or assignment of work" but has limited it to employees to simplify implementation for businesses at this time.
7200(a)	280, 281, 282, 577, 1128,	Comment recommends revising this provision so that ADMT requirements apply only to profiling that results in legally significant decisions. The proposed	The Agency disagrees with this comment. The extensive profiling and training thresholds are within the Agency's authority and are consistent with, and

DRAFT

	1552, 1559, 1560, 1565, 1571, 1596	regulations unnecessarily mandate ADMT requirements for all profiling activities, even when these do not result in legally significant decisions, such as financial, housing, or employment decisions. This broad approach creates excessive burdens for businesses, particularly since some impacts on consumers are speculative. The ADMT requirements should not apply to extensive profiling or training. At a minimum, the profiling for behavioral advertising threshold should be removed, or the notice requirements should be tailored to the reduced risk and different circumstances of advertising. Further, there should not be an opt-out right to all behavioral ads as it conflicts with the statutory opt-out framework that is limited to CCBA. As a final fallback, the rules should be clear that any opt out that applies to behavioral ads is limited to targeting ads based on inference preferences from consumers based on their personal data. The draft rules potentially sweep in contextual ads since the definition of behavioral ads is not limited to activity "over time." Additionally, the proviso in the "behavioral advertising" definition makes it seem like measurement (e.g., attribution) could be covered as well. It unhelpfully copies some CPRA language, but without the additional context from the CPRA that clarifies that measurement is not in scope. Comment states that the regulations should at minimum not apply the access right to profiling for behavioral advertising. Comment also suggests striking the definition of "behavioral advertising." In addition, training is not decisionmaking or its substantial facilitation, and the CCPA already governs personal information used in training. Training would also be unnecessarily burdensome without improving consumer privacy, as the regulations already provide sufficient	further the intent and purposes of, the CCPA. (*See* Civ. Code § 1798.185(a)(15.)) The regulations are necessary and not unnecessarily burdensome. However, the Agency has revised this section to focus on the use of ADMT for a significant decision. The Agency also revised the definition of ADMT to focus on use without any human involvement, a higher-risk use of ADMT, and revised the definition of significant decision for clarity. Collectively, these revisions balance protections for consumers' privacy and simplifying implementation for businesses at this time. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. For example, the Agency has removed "access to" to simplify implementation at this time. The term "compensation" is reasonably clear, and the Agency does not believe it requires additional clarification or removal. In addition, AB 2013 applies to CA state agencies, not to businesses, and would not provide information to consumers about a business's use of ADMT or their rights to opt-out of ADMT or to access ADMT. To the extent the comment suggests that independent contracting opportunities and compensation should not be included, the Agency disagrees. The CCPA specifically includes independent contractors within its scope; thus, the regulations require businesses to provide independent contractors with the ability to opt-out of ADMT and access ADMT. However, the Agency has limited allocation or assignment of work to employees, to simplify implementation for businesses at this time.

		privacy protections. Furthermore, no other state privacy law or AI regulation treats model training as a high-risk activity, and California's recent AB 2013 already addresses disclosure requirements related to data. At a minimum, training should not trigger a Pre-use Notice. It will contribute to notice fatigue without reducing risk as consumers will struggle to understand this notice. Further, the draft rules already require AI/ADMT deployers (i.e., "users") to conduct risk assessments and companies may invest in accuracy/testing safeguards that better demonstrate trustworthiness. In addition, terms like "access to" services and "compensation" are too vague and should be clarified or limited.	
Previous 7200(a)(1)	226, 577, 1856	Comment suggests that the definition of significant decision should be clarified. Specifically, § 7200(a)(1) should be revised to: (1) remove "access" from the definition of "significant decision" and (2) clarify that significant decisions are those with material, legal, or similarly significant effects on a consumer. Comment also opposes the inclusion of independent contracting and work allocation, as these decisions are often routine business operations rather than legally significant choices.	The Agency disagrees with this comment. However, the Agency has revised the definition of "significant decision" to provide additional clarity and removed "access to" from the definition. As revised, the definition is consistent with approaches taken in other jurisdictions, such as the EU and Colorado, and provides greater clarity about what decisions are included than the language suggested by the comment. With respect to independent contracting and work allocation, the CCPA explicitly provides privacy protections to employees and independent contractors, and provides consumers with rights to access and opt-out of ADMT. However, the Agency has limited allocation or assignment of work to employees, to simplify implementation for businesses at this time.
Previous 7200(a)(1)	393	Comment states that while § 7200(a)(1) properly clarifies that exempt data is out of scope, similar language is missing in Articles 9, 10, and 12, leading to potential regulatory conflicts. The regulation should	The Agency disagrees with this comment. However, the Agency has removed references to the CCPA's data-level exemptions in the definition of "significant decision" as unnecessary because the CCPA is reasonably clear in addressing which data are subject

		ensure consistency across all articles to prevent misinterpretation.	to the CCPA. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA, which applies to all of the regulations.
Previous 7200(a)(1)	338, 535, 664, 753, 1499, 1606	Comment finds the definition of "significant decision" problematic, as vague language could unintentionally expand regulatory scope and sweep in low-risk activities. Comment recommends aligning the definition with existing privacy norms that focus on decisions with material legal or similarly significant effects. The definition should focus on high-risk activities, not entire industries. Comment suggests limiting employment-related "significant decisions" to hiring, promotion, demotion, suspension, and termination, aligning with other jurisdictions. Comment also recommends "credit or lending decision" instead of "financial or lending services," and "diagnostic, planning, or care decision, patient monitoring and engagement" instead of "healthcare services." Comment also argues that the regulations should include more examples of what constitutes a "significant decision." While some examples are given, other contexts like financial services, housing, and healthcare lack examples, which could cause confusion and under-protection of consumers. One comment suggests pulling examples from the ACLU's letter on Executive Order N-12-23.	The Agency disagrees with his comment. However, the Agency has revised the definition of "significant decision" to provide additional clarity for businesses, and to further simplify implementation for businesses at this time. This includes providing additional clarity regarding financial or lending services, housing, and healthcare services. These requirements are appropriate to California and no further clarification is needed. As revised, the definition is consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. In addition, the definition focuses on decisions that present significant risk to consumers' privacy, not specific industries or whether it is a routine operation. With respect to employment-related decisions, the CCPA explicitly provides privacy protections to employees and independent contractors, and provides consumers with rights to access and opt-out of ADMT. However, the Agency has limited allocation or assignment of work to employees, to simplify implementation for businesses at this time.
Previous 7200(a)(1)(B)(ii)	875, 932	Comment suggests that for purposes of determining when a business's use of ADMT is subject to regulations, mere "allocation or assignment of work" should not constitute employment, independent contracting opportunities, or compensation. Comment argues that the inclusion of ADMT used for "allocation and assignment of work" under § 7200(a)(1)(B)(ii) is unnecessary and could restrict businesses' ability to	The Agency disagrees with this comment. The CCPA explicitly provides privacy protections to employees and independent contractors. The Agency has determined that a business's use of ADMT to allocate work presents significant risk to consumers' privacy and has accordingly retained it in the revised definition of "significant decision." The regulations focus not on whether the ADMT is part of "routine

		efficiently manage their workforce. Routine business decisions, such as scheduling and task assignment, should not be classified as "employment opportunities" or compensation decisions.	business operations" but on further protecting consumers' privacy, consistent with the CCPA.
Previous 7200(a)(2)	172, 665, 923, 1049, 1493, 1741, 1873	Comment states that the definition of "extensive profiling" under § 7200(a)(2)(C) is problematic due to its broad nature and vagueness. Comment is particularly concerned that "behavioral advertising" is included in this definition, as it includes first-party targeting activities that are not traditionally considered high-risk and are routine and non-invasive. The regulations threaten the digital-advertising ecosystem by conflating behavioral advertising with consequential decisionmaking systems. Behavioral advertising involves low-risk, often anonymized processes, not decisions that significantly affect consumers. Small businesses stand to lose the most from these regulations, as many rely on first-party and targeted advertising to reach niche markets in a cost-effective manner. Comment suggests deleting in its entirety, or including as follows: "For extensive profiling of a consumer. For purposes of this Article, 'extensive profiling' means any of the following to the extent the relevant observation or profiling involves systematic use of information that is not subject to the exceptions set forth in Civil Code §§ 1798.145, subdivisions (c)-(g), or 1798.146, subdivisions (a)(1), (4), and (5)[.]" Comment also suggests specifying that the imposition of requirements when a business uses ADMT for "profiling a consumer for behavioral advertising" in § 7200 (a)(2)(C) applies only to third-party behavioral advertising.	The Agency disagrees with this comment. The regulations are not broad, vague, or unduly burdensome. However, the Agency has revised the regulations to remove the extensive profiling threshold, to simplify implementation for businesses at this time.

DRAFT

Previous 7200(a)(2)(A)–(C)	1553, 1554, 1555, 1721	Comment believes that these provisions should be limited in scope, and that "or profiling" should be removed from subsection (a)(3)(C).	The Agency disagrees with this comment. However, the Agency has revised § 7200 to focus on the use of ADMT for significant decisions and revised the definition of ADMT to address the higher-risk use of ADMT without any human involvement.
Previous 7200(a)(3)	173	Comment suggests deleting in its entirety, or revising as suggested: "Processing consumers' personal information to train automated decisionmaking technology that is designed to be used for any of the following (but excluding the processing of personal information that is subject to, or the training of automated decisionmaking that is designed to be used with personal information that is subject to, one or more exceptions set forth in Civil Code Sections 1798.145, subdivisions (c)-(g), or 1798.146, subdivisions (a)(1), (4), and (5))[.]"	The Agency disagrees with this comment. However, the Agency has revised § 7200 to focus on the use of ADMT for significant decisions and revised the definition of ADMT to address a higher-risk use of ADMT without any human involvement. The Agency has 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 cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
Previous 7200(a)(3)	1110, 1174, 1206, 1303, 1360, 1556, 1765, 1840, 1997, 2018, 2019	Comment asserts that § 7200(a)(3) inappropriately includes "training ADMT" as a form of automated decisionmaking. Comment argues that training AI should not fall under the scope of the ADMT regulations because training AI does not involve making consequential decisions about consumers. The rule improperly regulates AI development rather than its deployment, contrary to the CCPA's purpose. Model training should not be subject to the same rules as AI systems making actual decisions because it does not present direct privacy risks to consumers. The regulations essentially create a right to opt-out of ADMT training data. This is a different opt-out and unnecessarily hamstrings startups that are developing their own ADMT applications. It could reduce accuracy and increase bias, and will make it impossible to maintain representative training data that does not	The Agency disagrees with this comment. The ADMT regulations are within the Agency's authority, consistent with the CCPA, and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(15).) The regulations also do not overlook CCPA's exemptions or its clarification that businesses are not required to reidentify or otherwise link information in the ordinary course of business, is not maintained in a manner that would be considered personal information. The CCPA is reasonably clear in addressing which data are subject to the CCPA. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The regulations would not increase bias, reduce accuracy, undermine compliance efforts, or be unduly burdensome. Rather, they would protect consumer privacy while providing flexibility for businesses to come into compliance.

		unintentionally discriminate against those groups whose representation in the dataset is skewed by the optouts. This would perversely be the case if the discriminated data subjects have themselves refrained from opting out, adding to the potential injustice. The ADMT training requirements also overlook explicit exemptions in the statute, such as the explicit recognition in the statute that "publicly available information" does not constitute personal information and that businesses are not required to relink information maintained separately in the ordinary course of business. The regulations also do not reflect the technical realities of how ADMT training works in practice. For example, much of the data used for ADMT training is sourced from datasets that are publicly available, and therefore, out of the scope of the CPPA's authority. Additionally, the regulations should recognize the statutory language that deidentified and aggregated data used for ADMT training is not subject to requirements. Comment claims that training data is aggregated and does not directly impact individual consumers. Comment argues that the opt-out requirement for ADMT use in training models poses significant issues for financial service providers. Lenders rely on large datasets to refine underwriting models and assess risk. If required to delete data used for training models, compliance costs would rise, potentially reducing the effectiveness of risk assessments. In addition, the regulations would undermine businesses' ability to protect the safety and security of consumers. Comment argues that the ADMT requirements should not apply to the training of systems that are capable of being used to establish	However, the Agency has deleted the training ADMT threshold from Article 11 and has revised § 7200 to focus on the use of ADMT for significant decisions to simplify implementation at this time.

		individual identity. Comment states that this provision should be limited in scope.	
7200, 7220	362, 581, 713, 890, 955, 1188, 1192, 1285, 1376, 1396, 1397, 1460, 1633, 1766, 1999	Comment argues that the ADMT requirements for businesses, including to provide a Pre-use Notice before processing personal data using ADMT, exceeds the Agency's legal authority and raises First Amendment concerns. For example, the Pre-use Notice and responses to access requests must include the "intended output" of this technology and "how the business plans to use the output." These explanations about the business' intent and judgments about its process reflect expressive content. The regulations also require a business that trains ADMT to make available documentation, which constitutes compelled speech. Specifically, even though the regulations style these disclosures as "facts" necessary for the recipient business to conduct its risk assessment, such disclosures require a subjective determination by the business, including about any "requirements or limitations" for the permitted use of the ADMT. To the extent that there is a compelling interest in facilitating the disclosure of information, the CPPA has not established that the required documentation is a narrowly tailored means of achieving that end. Further, the notice requirements provide little benefit in low-risk scenarios and can overwhelm consumers because of the multiple notices already required under the CCPA and the length of these notices. In addition, these requirements diverge from other privacy statutes that require a single, easy-to-locate privacy policy. The CPPA should remove the prescriptive Pre-use Notice requirements that are out of step with notice requirements under other privacy statutes, create ambiguity for businesses, run counter to the goal of	The Agency disagrees with this comment. The regulations implement a state law that tasks the Agency with its implementation. The Agency does not have the authority to deem a state law invalid or in conflict with constitutional provisions, nor does it believe that the regulation violates the First Amendment. The ADMT regulations, including the Pre-use Notice requirements, are within the Agency's authority and are necessary to ensure that consumers have relevant information about use the of ADMT to meaningfully exercise their CCPA rights. They also harmonize with other privacy laws, which similarly require transparency to consumers, while furthering the intent and purposes of the CCPA and providing clarity to businesses about the scope of their obligations. The requirements are not ambiguous or confusing, but rather provide clear requirements about what information must be provided to a consumer. In addition, it is unlikely that consumers will have notice fatigue from the Pre-use Notice. It is only required in limited circumstances, and businesses also have flexibility in providing the Pre-use Notice as part of a Notice at Collection, which reduces concerns about overwhelming consumers with notices. Moreover, with respect to third parties, the regulation is clear. The Pre-use Notice requirements apply to a "business" that is using ADMT.

		providing meaningful transparency to consumers by contributing to notice fatigue, and contribute to consumer confusion. The requirement should be deleted entirely or be limited to use cases subject to access and opt-out rights. Additionally, the rules lack clarity on how third parties can comply, as they often do not interact with consumers directly. The Agency should either remove this requirement or provide alternative compliance methods for third parties, similar to the California Data Broker Registry.	
7201	257, 260, 1937	Comment argues that the regulations are unclear as to what is required for compliance when evaluating ADMT systems used in employment decisions for non-discrimination safeguards, or who should conduct evaluations. Comment suggests deleting this section. Physical profiling is already covered by "profiling." Consumers already have the right to understand what is happening, what the logic involved is, the likely outcome, and then the right to opt out.	The Agency disagrees with this comment. The regulation is reasonably clear based on the plain meaning of the word(s), and is not duplicative with other requirements. However, the Agency has deleted § 7201, which imposed requirements for physical or biological identification or profiling, to simplify implementation at this time.
7201	827	Comment affirms that bias mitigation should occur for protected categories, intersectionalities, and vulnerable populations and be documented in a data transparency document that is available for independent third-party audit. Comment also recommends prohibiting AI and ADMT technologies that are unable to either have ground truth validation or affirmation by the impacted party of the inferential conclusions and lack causal hypothesis and construct validity, such as emotion-recognition systems.	The Agency agrees in part with this comment, to the extent it supports further protections for consumers' privacy. Nevertheless, the Agency has deleted § 7201, which imposed requirements for physical or biological identification or profiling, to simplify implementation at this time. With respect to prohibiting the use of certain technologies, this does not appear to be a comment on the proposed action.
7201	1459	Comment suggests deleting this section.	The Agency has deleted § 7201, which imposed requirements for physical or biological identification or profiling, to simplify implementation at this time.

7201	1510	Rather than relying only on heightened risk reporting, comment urges the Agency to impose per se bans on high-risk activities such as predictive policing, emotional recognition, and facial surveillance. These activities, even when undertaken by private vendors, carry excessive risks of discrimination and harm.	The Agency disagrees with this comment. With respect to the activities cited by the comment, to the extent a business is engaging in these activities using consumers' personal information, the business must comply with the CCPA's requirements, including providing relevant privacy disclosures and rights mechanisms and complying with the requirements in § 7002. The Agency has removed the evaluation requirements in § 7201 to further simplify implementation at this time. However, a business must still conduct a risk assessment when using ADMT for a significant decision and provide relevant opt-out and access mechanisms for consumers. The Agency does not believe that additional regulations are necessary at this time.
7201	1632	Comment argues that this section exceeds the Agency's regulatory authority. This rule does not contemplate that ADMT would be involved in the identification or profiling, or even that its use would be limited to when a decision is made about an individual.	The Agency disagrees with this comment. The ADMT regulations are within the Agency's authority and further the intent and purpose of the CCPA. However, the Agency has deleted § 7201, which imposed requirements for physical or biological identification or profiling, to simplify implementation at this time.
7201, 7221(b)	593, 671, 754, 831, 1088, 1164, 1237, 1275, 1375, 1609, 1638, 1714, 1715,	Comment supports the safety, fraud prevention, and safety exemption, but suggests it is too narrow and should be bolstered. The Agency should ensure that the protective activities included in the exemption are sufficiently broad to ensure that businesses are not forced to provide opt outs or other rights as to activities that serve important security and safety goals. For example, § 7221(b)(1)(B) should be strengthened to clarify that the opt out right does not apply to activities that are aimed "to resist, prevent, and detect, malicious, deceptive, fraudulent, or illegal actions directed at the business and to prosecute those responsible for those	The Agency disagrees with this comment. The security, fraud prevention, and safety exception has been removed from § 7221(b) because it is no longer necessary. The Agency modified the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. However, the Agency

	1716, 1898	actions; or […].” Additionally, fraud and security exceptions should be expanded to cover not only malicious actions “directed at the business” but also the business’ customers and should apply to training ADMT – bad actors should not be able to opt out of their data being used to train the very systems that seek to detect them. Instead, processing to detect, prevent, resist, investigate, and prosecute such activities should be exempt regardless of the target of the attack — whether consumers, other businesses, or government organizations. Comment proposes exempting uses for security, fraud prevention, and safety from all ADMT-specific obligations, except § 7201, and recommends that the Agency make corresponding numbering changes to the remaining exemptions to reflect the removal of § 7221(b)(1). Comment also suggests deleting the term “profiling” in § 7201(a) and adding language about using ADMT to evaluate biometrical identification. Comment suggests including protection of personal property. Comment also raises concerns that the opt-out framework under § 7221 is overly restrictive and could disrupt business operations. The “necessary to achieve” standard for security, fraud prevention, and safety is too strict and ignores how businesses use ADMT effectively. Comment suggests a more flexible standard, such as “solely used for” these purposes, or a broader standard. Comment suggests that AI in security helps analyze risks faster, but the proposal limits these benefits. The narrow exemption to the ADMT opt-out for security, fraud prevention, and safety is also out of step with other U.S. privacy statutes (Colorado, Connecticut, Florida, Indiana, Iowa, Montana, Texas and Virginia), which recognize a broader exemption for fraud, security, and consumer safety. Comment states that	revised the regulations to expand the security, fraud-prevention, and safety exceptions elsewhere within the regulations, to cover malicious activities directed at consumers. (*See* §§ 7220(d)(2)(B), 7222(c)(2)(B), 7027(m)(3).) The Agency also revised the regulations to clarify that a business is not required to include certain security, fraud prevention, or safety information when providing required information in Pre-use Notices and in responses to consumers’ access ADMT requests. (*See* §§ 7220(d), 7222(c).) Additionally, the Agency deleted § 7201, which imposed requirements for physical or biological identification or profiling, to simplify implementation at this time. With respect to other states’ exceptions, the comment appears to refer to those states’ general statutory exemptions, not to exceptions to a consumer’s right to opt out. In addition, comment’s recommendation regarding statutory exceptions is not necessary. The CCPA’s statutory exemptions apply to the regulations, The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Whether an exemption applies is a fact- and context-specific determination. Further, with respect to disclosures about the use of ADMT tools, the Pre-use Notice requires disclosures of the use of ADMT for a significant decision. This addresses comment’s suggestion to require disclosures regarding the use of ADMT tools.

		expanding the exemption to include all ADMT-related rules (including risk assessments) would align with laws like the Colorado AI Act. In addition, comment believes that the scope of this exception needs clarification in the HR context where ADMT often serves multiple purposes that may qualify for this exemption. Additionally, comment suggests adding "§ 7221 (b)(8): This section shall not restrict a business's ability to retain information or comply with any other legal obligation as set forth in Civil Code section 1798.105, nor restrict compliance with medical record laws as set forth in the Health and Safety Code." Comment also suggests the following modifications in § 7200(b): "Notwithstanding subsection (a), use of ADMT solely for the security, fraud prevention, or safety purposes listed below ('security, fraud prevention, and safety exception') is exempt from sections 7220,7221, and 7222 of these regulations: (1) To prevent, detect, resist, and investigate security incidents that compromise the availability, authenticity, integrity, or confidentiality of personal information; (2) To prevent, detect, resist, and investigate malicious, deceptive, fraudulent, or illegal actions and to prosecute those responsible for those actions; or (3) To ensure the safety of natural persons." Comment also recommends requiring the disclosure of the use of ADMT tools to students or employees, contractors, or gig-workers.	
7220	215	Comment suggests that the requirements for additional pre-use disclosures specific to ADMTs creates unnecessary hurdles, especially for existing customers who already consent to services.	The Agency disagrees with this comment. The notice requirements would not impede consumers, because they ensure that consumers have meaningful information prior to exercising their CCPA opt-out and access rights. Nevertheless, the Agency has revised the regulations to further simplify implementation for businesses at this time, including enabling businesses

			to include the Pre-use Notice with the Notice at Collection.
7220	283, 667, 1121, 1187, 1345, 1557	Comment argues that the Agency lacks statutory authority to require businesses to provide Pre-use Notices before using ADMT. The CCPA only allows businesses to disclose "meaningful information about the logic" behind ADMT in response to access requests, not through Pre-use Notices. The Pre-use Notice requirement contradicts this by imposing an overly complex, redundant, and unnecessary disclosure obligation. If the California electorate intended to permit the CPPA to issue rules on Pre-use Notices for ADMT, it would have been clear on this point. The statute expressly states when prior notice is required at or before collection and does not authorize the CPPA to amend the notice-at-collection rules to specifically address ADMT or authorize other ADMT Pre-use Notices. At minimum, these requirements should be aligned with existing CCPA language or limited to instances where ADMT use is already subject to access and opt-out rights. Additionally, when customer rights such as access or opt-out do not apply, businesses should not be obligated to provide Pre-use Notices. § 7220(a) should align with the exceptions outlined in §§ 7221(b) and 7222(a)(1) to avoid creating unnecessary risks, such as undermining consumer or business security.	The Agency disagrees with this comment. The Pre-use Notice requirements are within the Agency's authority and are necessary to ensure that consumers have relevant information about use the of ADMT to meaningfully exercise their CCPA rights. The regulations were also revised to provide further clarity to businesses regarding the relevant information to provide consumers about the use of ADMT, and to enable further flexibility in providing these notices, such as combining it with a Notice at Collection. The Pre-use Notice is not redundant, rather it ensures that consumers have meaningful information about use the of ADMT with respect to them when they are exercising their CCPA rights. With respect to security and fraud prevention, a Pre-use Notice is not required to include certain information regarding security, fraud prevention, and safety, as set forth in § 7220(d)(2). The Pre-use Notice requirements are limited to when consumers exercise their relevant CCPA opt-out and access rights, subject to certain exceptions. Comment's recommendation to remove Pre-use Notice requirements when an exception applies misreads the regulations. A business that is subject to an opt-out exception must still provide relevant disclosures in the Pre-use Notice, including, for example, the exception it is relying on to not provide the opt-out or how to submit an appeal of a significant decision. In addition, a business must always provide the information required in § 7222(b) in response to a request to access ADMT. However, it is not required to provide trade secret or certain security, safety, and fraud prevention information set

			forth in § 7222(c) when providing those disclosures. It is unclear how a Pre-use Notice will undermine security. The regulations explicitly provide an exception for disclosing certain security information in § 7220(d)(2).
7220	440	Comment supports the disclosure requirements in Article 11 (§ 7220), advocating that businesses using ADMT must provide a Pre-use Notice to consumers. This notice should inform consumers about the business's use of ADMT and their rights to opt out and access ADMT.	The Agency agrees with this comment and notes comment's support.
7220	583, 1841	Comment suggests that rather than mandating a separate Pre-use Notice, ADMT-related disclosures could be incorporated into privacy notices, avoiding redundancy and notice fatigue while maintaining transparency. Comment proposes either removing the requirement or incorporating it into existing privacy notices. If retained, comment suggests that-low risk use cases be clearly excluded, and that the contents are simplified.	The Agency disagrees with comment. The notice requirements ensure that consumers have meaningful information to exercise their CCPA rights. In addition, the notice requirements provide businesses with flexibility in how they are consolidated or included with the Notice at Collection and have simplified what information must be provided to the consumer. The regulations have also been revised to focus on the use of ADMT for significant decisions at this time.
7220	584	Comment suggests adding "§ 7220(e): The requirements set forth in this Article apply to processing activities created or generated 24 months after the final regulations are published, and are not retroactive to any processing activities created or generated before that time."	The Agency disagrees with this comment. Comment's recommendation is less effective than the regulation at protecting consumer privacy, because it would limit the ability of consumers to exercise their CCPA rights. The Agency has added § 7200(b) to provide businesses until January 1, 2027 to come into compliance with Article 11.
7220	781	Comment suggests that the regulations should require Pre-use Notices to include risks posed by ADMTs and alternative options in § 7220. This would help consumers, especially vulnerable groups like workers, make informed choices.	The Agency disagrees with this comment. The notice requirements ensure that consumers have meaningful information to exercise their CCPA rights. They also provide a flexible, performance-based standard for businesses regarding how to provide the required

			information. In addition, the Agency has revised the ADMT requirements, including focusing on significant decisions and providing additional clarity regarding what information must be disclosed to consumers, to further simplify implementation for businesses at this time. The Agency has determined additional disclosure requirements are not necessary at this time.
7220	819, 820, 821	Comment suggests that pre-use notifications of ADMT should apply to work and education even when the ADMT is for safety, security, and fraud detection purposes per § 7221(b)(2), as a result of an existing appeals process for human review per § 7221(b)(2), or as a result of usage of the ADMT in automated employment decisionmaking per §§ 7221(b)(3), 7221(b)(4), and 7221(b)(5).	The Agency disagrees with this comment. The Agency has revised Article 11 to remove the work/educational profiling uses of ADMT, to simplify implementation for businesses at this time. Comment also misreads the regulations. A business must still always provide a Pre-use Notice if it is using ADMT for a significant decision. However, the business is not required to include certain safety, fraud prevention, and safety information in that notice.
7220	1165, 1208	Comment states that § 7220 requires businesses using ADMT to provide a Pre-use Notice to consumers. However, this does not account for businesses that do not have a direct relationship with consumers (e.g., developers or home security providers that interact only with the system purchaser, not visitors). Furthermore, requiring developers to specify the intended use of AI systems is unrealistic since developers do not always control how the AI is deployed.	The Agency disagrees with this comment. A Pre-use Notice must be presented in the manner in which the business primarily interacts with the consumer. The regulation is reasonably clear and applies a performative standard that gives businesses flexibility to craft a method that best fits their businesses' operations. The regulations have also been revised to enable businesses to provide the Pre-use Notice in the Notice at Collection and focus on businesses' use of ADMT to make a significant decision concerning a consumer. Further, proposed § 7220(c)(1)(A) is not infeasible. However, the Agency has removed this requirement to further simplify implementation for businesses at this time.
7220	1908	Comment supports stronger rights around ADMT transparency, access, appeal, and opt-out. While the	The Agency disagrees with this comment. The term "plain language" is reasonably clear and provides a

		proposed rule requires a "Pre-use Notice" under § 7220, these rights are subject to exceptions that weaken them. Comment recommends that the Agency incorporate a concrete, explicit definition of "plain language" to ensure that the required disclosures are fully accessible, and meaningfully increase consumer awareness of their rights. Such a requirement already exists in the Civil Code, but is currently-narrowly scoped to products that handle genetic information. Comment recommends that the Agency replicate the disclosure standard of Civil Code § 56.18(a)(6).	flexible, performance-based standard for businesses when providing disclosures to consumers. Similarly, the exceptions to the Pre-use Notice requirements ensure that businesses provide meaningful information to consumers about their use of ADMT without compromising certain security, fraud prevention, or safety information or disclosing trade secrets. The Agency does not believe that additional modifications are not necessary at this time.
7220(a)	859	Comment suggests that the Pre-use Notice requirements should not apply to a business that only uses ADMT with respect to personal data that is exempt from the CCPA pursuant to § 1798.145, e.g., GLBA, HIPPA, FCRA, etc. Placing this requirement on such businesses will likely lead to consumer confusion while imposing additional compliance burdens on businesses without any countervailing benefits for consumers.	The Agency disagrees with this comment. The exemptions provided under the CCPA, including those for GLBA, FCRA, and HIPAA-governed data, are already explicitly stated in the statute. There is no requirement to reiterate these exemptions in the regulations, as doing so could create unnecessary complexity or confusion. The Agency has accordingly removed references to the exemptions in the definition of "significant decision" to avoid similar confusion about when the exemptions apply. A business has Pre-use Notice obligations when it uses ADMT to make a significant decision concerning a consumer.
7220(c)	828	Comment suggests that the words "capable of being used" be replaced by "the business must identify permitted usage of ADMT or AI in terms of Scope, Nature, Context, and Purpose" and document permitted usage in applicable contracts.	The Agency disagrees with this comment. The Agency has revised Article 11 to remove training uses, to simplify implementation for businesses at this time.
7220(c)	933, 1313, 1494	Comment argues that the Pre-use Notice requirements in § 7220(c) are burdensome and risk exposing trade secrets and confidential information. Businesses should not be required to disclose proprietary ADMT logic or	The Agency disagrees with this comment. A Pre-use Notice is not burdensome and does not require a business to include trade secrets or certain information regarding security, fraud prevention, and

		intended outputs, as required by §§ 7220(c)(5)(A) and (B). Additionally, a broader exemption should be introduced for fraud detection and security tools to prevent bad actors from exploiting disclosed ADMT details.	safety in the notice, as set forth in § 7220(d) of the regulations. The Agency does not believe that additional exemptions are necessary at this time.
7220(c)(1)	284, 365, 1613	Comment recommends removing the explicit prohibition on using the phrase "to improve our services," as this language can serve as part of a legitimate description of businesses' use of ADMT. Comment argues that this prohibition may present compliance difficulties and could inadvertently force disclosure of sensitive operational details.	The Agency disagrees with this comment. The regulation is clear and has been revised to add further clarity regarding why generic terms are not helpful for consumers in disclosures. The Pre-use Notice requirement also contains exceptions as needed for trade secrets and certain security, fraud prevention, and safety information, as set forth in § 7220(d) of the regulations. This ensures businesses can comply with the Pre-use Notice requirements while providing appropriate protections for trade secrets or certain security, fraud prevention, and safety information.
Previous 7220(c)(1)(A)	582	Comment suggests that the pre-use requirement is more stringent than comparable privacy laws. Additionally, § 7220(c)(1)(A) requires businesses to list all possible uses of an ADMT system, which may be infeasible, particularly for AI developers who lack control over downstream usage.	The Agency disagrees with this comment. The Pre-use Notice harmonizes with other laws while furthering the purposes of the CCPA and providing clarity to businesses about their obligations. Proposed § 7220(c)(1)(A) is not infeasible. However, the Agency has removed this requirement to further simplify implementation for businesses at this time.
7220(c)(3)	1634	Comment states that requiring businesses to disclose opt-out exceptions at the pre-notice stage is inconsistent with other CCPA rights and too nuanced for advance notice.	The Agency disagrees with this comment. The disclosure requirements ensure consumers understand why they are not being given the ability to opt-out, and provide relevant information, such as how to exercise the ability to appeal.
7220(c)(5)	670	Comment argues that the requirement for a Pre-use Notice in contexts such as behavioral advertising or fraud and security tools is especially problematic. Behavioral advertising typically does not involve	The Agency disagrees with this comment. The Pre-use Notice ensures that consumers have meaningful information about use the of ADMT with respect to them when they are exercising their CCPA rights. In

		significant decisions or consumer impacts that justify heightened transparency. Comment urges the Agency to consider the wisdom of continually requiring additional notices to be drafted.	addition, the Agency has revised the ADMT requirements, including focusing on significant decisions and providing additional clarity regarding what information must be disclosed to consumers, to further simplify implementation for businesses at this time.
7220(c)(5)	829	Comment affirms that transparency and explainability are foundational elements of the responsible deployment of ADMT and AI. Comment further recommends that clear and plain language explanations should satisfy legal obligations and fundamental human rights. Explainability need never include intellectual property or other proprietary information. However, basic logic and clear and plain language explanations would never constitute IP or proprietary information and arguments made to the contrary are red herrings.	The Agency agrees with this comment and notes comment's support.
7220(e) [previously 7220(d)]	999	Comment suggests merging Pre-use Notices with the Notice at Collection under § 7012 to streamline compliance obligations. Comment suggests adding language to § 7220(d): "and may be included in the Notice at Collection, § 7012."	The Agency agrees in part with this comment. However, the comment's proposed language does not provide sufficient guidance to a business about what requirements a Pre-use Notice must meet when provided in a Notice at Collection. The Agency has provided guidance in the regulations that businesses can provide a Pre-use Notice in its Notice at Collection, provided that the Notice at Collection complies with, and includes the information required by, §§ 7220(b)-(c).
7220, 7222	261, 285, 362, 365, 567, 668, 669, 1204, 1558, 1614,	Comment argues that the regulations present significant challenges in addressing the nuanced differences between AI model types. They impose an explainability requirement that may not be practical for many complex AI models, which are often not fully explainable despite their utility. They do not benefit consumers and could result in complex and unclear	The Agency disagrees with this comment. The regulations are within the Agency's authority and ensure that consumers have meaningful information about use the of ADMT when they are exercising their CCPA rights. They also provide a flexible, performance-based standard for businesses regarding how to provide the required information. In

	1635, 1722, 1766, 1768, 1846, 1849, 1851	notices and notice fatigue. They are also overly prescriptive and should provide greater flexibility to businesses on the content and format of the notices. They will disincentivize innovation by creating burdensome technical and disclosure requirements. The regulations also fail to explain how the disclosures would function. Comment suggests alternative approaches, such as human review and rigorous testing, to mitigate risks. The draft regulations also conflict with the CCPA by requiring disclosures that could infringe on trade secrets. The exception under § 7220(c)(5)(C) is too narrow. This is particularly important in the HR context, because HR deals with not only employee confidential data, but also beta and pilots for products that should be excluded as confidential business/trade secret information. Further, §7220's requirement presents challenges in the employment context where ongoing relationships exist. While consolidated notices are permitted, employers still risk overwhelming employees with disclosures. In addition, the regulations function as an AI Impact Assessment framework, rather than mere access rights. Comment also requests confirmation that these requirements will not be retroactive and will exclude third parties. Comment suggests striking § 7220(c)(5). Comment opposes the Pre-use Notice requirements in § 7220, arguing they are similar to the EU's opt-in standards and exceed the CCPA's opt-out framework. Comment suggests the Agency striking § 7220 and the corresponding reference in §§ 7010(c) and (d) entirely. If the Agency determines some more limited form of ADMT notice falls within its legislative mandate, comment recommends it: (1) remove the detailed obligations set forth in the draft, allowing businesses to communicate with consumers in ways that match their	addition, the Agency has revised the ADMT requirements, including focusing on significant decisions and providing additional clarity regarding what information must be disclosed to consumers, to further simplify implementation for businesses at this time. Further, the Pre-use Notice and responses to access requests do not require the inclusion of trade secrets. (*See, e.g.*, § 7220(d)(1).) In addition, it is unlikely that consumers will have notice fatigue from the Pre-use Notice. It is only required in limited circumstances, and businesses also have flexibility in providing the Pre-use Notice as part of a Notice at Collection, which reduces concerns about overwhelming consumers with notices. The regulations regarding timing and which entities are subject to compliance are clear. For example, if a business is using ADMT to make a significant decision before January 1, 2027, it must be in compliance with Article 11 no later than January 1, 2027. With respect to third parties, the regulation is clear that the Pre-use Notice requirements apply to a "business" that is using ADMT.

		business practices, and (2) limit the applicability of the Pre-use Notice to scenarios in which businesses use ADMT to make significant decisions. Comment further urges the Agency to treat any required ADMT-specific notice as similar to other notices required under the CCPA, such as the notice of the consumer's right to opt-out of sale/sharing in § 7013 or to limit the use of their sensitive information in § 7014.	
7220, 7222	585	Comment suggests adding "§ 7220(f): Nothing in this article shall be construed as requiring a business to disclose trade secrets." Comment also suggests striking the notice for adverse significant decisions in § 7222, as it would be exceptionally burdensome to operationalize for low-risk use cases and would provide little benefit to consumers.	The Agency disagrees with this comment. The Pre-use Notice does not require the inclusion of trade secrets, as set forth in § 7220(d)(1). In addition, the adverse significant decision requirements are not overly burdensome and can be consolidated with existing notice processes. However, the Agency has removed the adverse significant decision requirements to further simplify implementation for businesses at this time.
7220, 7221	1050, 1236	Comment argues that while consumer opt-out rights are important, requiring a Pre-use Notice and opt-outs in dynamic settings (e.g., online marketplaces, automated content moderation) is impractical. It may also undermine user safety by delaying or limiting automated enforcement of platform guidelines. Comment also raises concerns that a Pre-use Notice and opt-out requirements could create excessive notifications, leading to user fatigue, similar to ineffective "cookie banner" regulations.	The Agency disagrees with this comment. The Pre-use Notice and opt-out requirements provide flexibility and are adaptable to a variety of use cases and contexts. They also do not undermine user safety. For example, the Pre-use Notice provides an exception for certain safety information. Both the Pre-use Notice and opt-out requirements have also been revised to focus on the use of ADMT for significant decisions, which further simplifies implementation for businesses. The regulations also enable businesses to combine the Pre-use Notices with a Notice at Collection, or to consolidate Pre-use Notices, which addresses comment's concern about excessive notifications and user fatigue.
7221	122	Comment argues that the proposed opt-out regulations would hinder businesses' ability to conduct	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations that govern

		personalized advertising and is outside the Agency's authority. This practice, such as sending targeted promotions based on past purchases, is seen as valuable by consumers and small businesses alike, and the regulations would require complex systems that could be technically unfeasible for many.	access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The regulations are within scope of this authority, and are not unduly burdensome or technically infeasible. However, the Agency has removed profiling for behavioral advertising requirements to simplify implementation for businesses at this time.
7221	216	Comment notes that the mandated opt-out mechanisms for ADMTs are redundant given existing regulations, such as universal opt-out mechanisms, and would impose unnecessary compliance costs.	The Agency disagrees with this comment. Existing opt-out mechanisms address the opt-out of sale or sharing and limiting the use and disclosure of sensitive personal information. § 7221 addresses the opt-out of ADMT and has been revised to focus on the use of ADMT for significant decisions. The opt-out requirements would not impose unnecessary compliance costs. The Agency has taken steps to reduce the burden of the regulations, including enabling businesses to leverage existing CCPA compliance processes to comply with § 7221.
7221	364, 591, 675, 1561, 1637, 2000	Comment states that the requirement to allow consumers to opt out of ADMT regardless of risk level is impractical and overly burdensome. The broad definition forces businesses to evaluate a vast range of systems for opt-out eligibility and requires businesses to disgorge previously collected information when a consumer opt out is operationally challenging and may be unworkable. Comment states that a blanket opt-out assumes ADMT is inherently harmful, disregarding its benefits like efficiency and reduced human bias. Expanding exceptions under § 7221(b) to include internal research, error resolution, effectuating product recalls, and routine operations would better align with consumer expectations, business needs, and other privacy laws. Comment also recommends requiring	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Thus, § 7200 identifies when the use of ADMT requires a consumer's ability to access and opt-out of that use of ADMT. The Agency has revised the definition of ADMT to focus on uses without any human involvement, a higher-risk use of ADMT, and has revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. The Agency has also made efforts to limit the burden of the regulations while implementing the CCPA. Additionally, the opt-

		verified requests to opt-out of ADMT. Comment argues that verification should be allowed in specific circumstances, such as admissions or employment screening, where a consumer may prefer that a business use ADMT because humans may have greater biases. Comment also recommends that § 7221(b)(1)(B) be clarified to exempt fraud prevention activities.	out requirements are clear. Once a consumer has opted out, a business must cease processing the consumer's personal information using that ADMT. This is a reasonable requirement to ensure consumers' opt-outs are honored. In addition, requiring verification would limit consumers' right to opt-out of ADMT and be inconsistent with other CCPA opt-out rights, thus, limiting businesses from leveraging their existing processes to meet ADMT opt-out requirements. (*See* §§ 7026(b)–(d), 7027(c)–(e).) The regulations provide consumers with a choice about whether they want to opt out of a business's use of ADMT, and enable businesses to present the consumer with the choice to allow specific uses of ADMT as long as the business also offers a single option to opt-out of all of the business's uses of ADMT. (See § 7221(i).) The proposed regulations balance privacy protections for consumers and flexibility for businesses regarding how to address consumers' concerns about the use of ADMT to make significant decisions about them. Further, the fraud exception has been removed because it does not apply when businesses use ADMT for a significant decision. Businesses may still deny fraudulent requests as set forth in § 7221(g). In addition, comment's recommended exceptions would be less clear and less effective than the regulations at protecting consumer privacy. Further, although the Agency strives for consistency with other privacy and laws when appropriate, it must comply with California law and adopt requirements appropriate to California. Additional exceptions to the opt-out right are not necessary at this time.

DRAFT

7221	502	Comment supports stronger privacy protections, particularly a categorical opt-out for behavioral advertising. Comment argues that behavioral advertising leads to invasive surveillance, discrimination, and consumer harm.	The Agency agrees with this comment, to the extent that it supports privacy protections for consumers. However, the Agency revised the regulations to remove the profiling for behavioral advertising threshold, to simplify implementation for businesses at this time.
7221	525, 543, 588, 1340, 1341, 1566, 1608, 1611, 1641	Comment opposes the consumer right to opt out of ADMT training data, arguing it could hinder businesses developing their own AI applications. Opt-out rights for training data also could introduce bias into AI models, restrict innovation and undermine data minimization, and undermine the development of fair, accurate, and safe ADMT. Regulators and technical experts recommend that companies develop and fine-tune ADMT systems based on training data that resembles the population within which the system will be deployed. Comment also states that data used in training is incidental. Moreover, any risks posed to consumers with respect to specific pieces of PI used by ADMT for training are adequately addressed through the existing correction right. Comment states that including "training" in § 7200(a)(3) is also impractical, since developers may not know the ADMT's exact capabilities at the training stage. Instead, developers should be encouraged to identify the range of applications suited or unsuited, and any applications or tasks considered inappropriate. Comment urges the Agency to issue guidance clarifying how businesses can comply with § 7221's opt-out rights when ADMT is trained on personal information. Since deleting data from certain models may not be feasible, developers should be permitted to implement technical solutions such as output filters. In some situations, businesses	The Agency disagrees with this comment. However, the Agency has revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. This includes removing the training ADMT threshold from Article 11. The regulations are reasonably clear how businesses must comply with consumers' requests to opt out of ADMT, and the Agency believes no further clarification is needed at this time.

		could fulfill opt-out requests by using manual alternatives to ADMT systems. § 7200 should exclude ADMT training uses. If that is not excluded, then the opt-out exceptions should apply to this use, in particular, the fraud and security exception under subsection (b)(1) and the evaluation exception under subsections (b)(3), (4), and (5). Businesses should be encouraged to evaluate whether the ADMT is discriminatory or working as intended and the best way to do that is to train on representative samples of data. If AI/ADMT training is not excluded entirely from Article 11, then another fallback should exclude or limit the right to opt out. Generally, for model training (especially for the largest models trained on internet-scale data), personal data included in the training corpus is incidental. Requiring implementation of an opt out process runs counter to data minimization best practices, as it may require individual identification. The preferred option would be to strike § 7150(b)(4) – AI/ADMT Training altogether. If not, amend § 7221(b) by striking (b)(6).	
7221	477, 509, 521, 542, 673, 1032, 1636	Comment states consumer opt-out rights would force businesses to redesign their services, restrict internal personalization efforts, disrupt standard practices like first-party advertising, and negatively impact small and minority-owned businesses that rely on targeted advertising. California could face broader economic consequences if businesses shift their advertising investments elsewhere. Comment opposes opt-out requirements for programmatic advertising, which create an uneven compliance burden, hinder competition, and interfere with legitimate business practices. Comment contends that the regulations impose impractical opt-out requirements on entities	The Agency disagrees with this comment. The requirements for profiling for behavioral advertising are reasonable, and would not be unduly burdensome on businesses. However, the Agency has revised the regulations to remove "profiling for behavioral advertising" from the regulations, to simplify implementation for businesses at this time.

		using programmatic advertising, disregarding common industry practices such as weekly updates to suppression lists. Comment argues that behavioral advertising should be excluded from ADMT's scope, or at least not subject to broad opt-out rights. The proposed rules impose more onerous requirements than existing ones under § 7013, despite lower risk. Comment also urges the Agency to allow businesses a reasonable timeframe (e.g., 15 days) to comply with opt-out requests.	
7221	506, 524	Comment suggests opt-out rights should only apply when profiling results in legally significant decisions, same as for public profiling. Comment opposes the creation of a consumer right to opt out of ADMT used for consumer profiling, arguing that this contradicts the CCPA's provisions.	The Agency disagrees with the comment. The ADMT regulations are consistent with the CCPA, are within the Agency's authority, and further the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT, including profiling. (*See* Civ. Code § 1798.185(a).) Nevertheless, the Agency revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time.
7221	548	Comment supports the regulations. Opt-out rights should be strong for harmful ADMT applications.	The Agency agrees with this comment and notes comment's support.
7221	586	Comment argues that ADMT enhances consumer experiences by providing efficient and data-driven services. Allowing opt-outs could diminish the value of these products and make them infeasible in some cases.	The Agency disagrees with this comment. The regulations do not diminish the value of businesses' products and provide flexibility for businesses, such as opt-out exceptions as necessary. Moreover, the CCPA directs the Agency to issue regulations governing opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency has also revised the definition of ADMT to focus on a higher-risk use of ADMT, which is a use without any human involvement; and has revised § 7200 to focus on the use of ADMT for significant

			decisions, to simplify implementation at this time. The regulations balance privacy protections for consumers and flexibility for businesses regarding how to address consumers' concerns about the use of ADMT to make significant decisions about them.
7221	589	Comment suggests adding another exception to avoid one-size-fits-all opt-outs that are confusing or misaligned with consumers' expectations. Comment proposes the following language as § 7221(b)(7): "The business's use of that automated decisionmaking technology is necessary to provide the online service, product, or feature requested by the consumer or the aspects of the online service, product, or feature with which the consumer is actively and knowingly engaged; or the business can demonstrate a compelling reason that the use of that automated decisionmaking technology does not pose a substantial privacy risk to consumers."	The Agency disagrees with this comment. The recommendation would be less clear and less effective than the regulations at protecting consumer privacy. The Agency has determined that additional exceptions are not necessary at this time.
7221	672, 881	Comment argues that the employment-related opt-outs should not be covered under consumer privacy laws since employment decisions already fall under labor regulations. Any employment opt-out should be eliminated entirely.	The Agency disagrees with this comment. The CCPA specifically includes employees and independent contractors within its scope. Article 11 provides these consumers with the ability to opt-out of the use of ADMT to make a significant decision about them, which includes employment decisions.
7221	1007	Comment argues that personalized advertising should not be covered under ADMT regulations, as it contradicts the CCPA definition of "cross-context behavioral advertising" and could harm small businesses by increasing advertising costs and complexity.	The Agency disagrees with this comment. The regulations are consistent with the CCPA, within the Agency's authority, and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(14)-(15).) However, the Agency has revised the regulations to remove the profiling for behavioral advertising threshold, to simplify implementation for businesses at this time.

7221	1051	Comment states that opt-outs for certain ADMT functions (such as recommendation algorithms) could degrade user experience and product functionality. Comment argues that if a person chooses to opt out of a certain ADMT that is inherent to the value of the product, then an opt out is legally effectuated by no longer using the product in question, and it would be unreasonable to consider that to be retaliation.	The Agency disagrees with the comment. To the extent the comment argues that the regulations should require consumers to stop using a business's product or service that relies upon ADMT, rather than require the business to provide consumers with the ability to opt-out from their use of ADMT, the Agency disagrees, because that would be inconsistent with the CCPA, which includes providing meaningful control to consumers over their personal information. The ADMT regulations balance protections for consumers' privacy and providing businesses with flexibility to come into compliance. With respect to retaliation, the existing regulations are reasonably clear about which practices violate CCPA's nonretaliation provision. (*See* Article 7.) The also Agency revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time.
7221	1120, 1284	Comment states that the regulations do not clarify whether the CCPA's commercial credit reporting exemption extends to ADMT opt-out rights. Comment argues that if commercial credit reporting data were subject to ADMT opt-outs, it could hinder business lending, fraud prevention, and regulatory compliance, making it more difficult and costly to assess business creditworthiness. Comment further states that if commercial credit data were removed from reports due to ADMT opt-outs, small businesses might struggle to secure financing, ultimately impacting economic growth and innovation in California.	The Agency disagrees with the comment. The CCPA and Article 11 already provide relevant exemptions for businesses' use of ADMT. Additional exemptions are not necessary. Businesses can, for instance, rely on the human appeal exception, if an opt-out is not feasible.
7221	1129	Comment opposes the proposal to introduce an opt-out for data processed using ADMT, arguing it could	The Agency disagrees with the comment. The Agency § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. The

		negatively impact publishers who rely on automation for content personalization and advertising.	ADMT regulations balance protections for consumers' privacy and providing businesses with flexibility to come into compliance.
7221	1500	Comment supports stronger opt-out rights for behavioral advertising, which go beyond the CPRA's protections limited to "cross-context" behavioral advertising. Comment argues that this stronger protection is necessary given the documented harms of behavioral advertising, including invasiveness, discrimination, and increased exposure to scams.	The Agency notes comment's support. However, the Agency has revised the regulations to remove "profiling for behavioral advertising" from the regulations, to simplify implementation for businesses at this time.
7221	1897	Comment concerned that the broad opt-out rights under §7221 could severely disrupt essential HR functions and create inequitable workplace situations. If employees opt out of AI-powered performance management systems, businesses would have to create and maintain parallel processes for opted out and non-opted-out employees, creating significant operational challenges and potential fairness issues. This burden is especially concerning for small to midsize businesses.	The Agency disagrees with this comment. The regulations provide businesses with relevant exceptions to the opt-out right, such as those for allocation and assignment of work decisions. This addresses comment's concerns about operational and fairness issues, and balances protect consumer privacy with providing flexibility for businesses to come into compliance.
7221	1919	Comment states that the regulations give consumers a right to opt out of ADMT if there's a significant decision or profiling, but if a business provides an appeal mechanism, it does not have to offer an opt-out. This is not feasible at scale and does not reflect how the real world works. It could allow consumers to opt out of contextual ads and could break the internet, and destroy the concept of moving the ad economy towards privacy-protective contextual ads. For example, these regulations could give consumers the right to opt-out of automated delivery scheduling software to deliver food or medications, booking software a hotel or airline that uses in quoting a price or making a reservation, and software that universities use to organize applications	The Agency disagrees with the comment. The Agency modified the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and § 7200, to focus on the use of ADMT for significant decisions to simplify implementation at this time. The regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. The regulations are scalable and would not be

		or not advance a candidate. Comment suggests alternative language with examples in § 7221 that makes an exception to opt-out where the ADMT is necessary to function, and to provide the consumer a good or service the consumer is requesting, as long as the ADMT is not used for profiling.	unduly burdensome on businesses. In addition, the comment's suggestion is not more effective or appropriate than the regulations at protecting consumer privacy.
7221	1938	The Agency should delete work or educational profiling and public profiling from this subsection.	The Agency agrees with this comment, to the extent it requests deletion of these thresholds from the opt-out requirements. The Agency has revised Article 11 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. The Agency has accordingly revised the opt-out exceptions. These revisions include removing references to "work or educational profiling" and "public profiling" from § 7221.
7221	1941	Comment suggests adding language such as: "If a business does not fulfill a consumer request to opt out pursuant to § 7221(b), the business shall inform the consumer of such action and include a detailed explanation of why the request was not fulfilled."	The Agency disagrees with this comment. The recommendation is unnecessary. The regulations already require a business that denies a request to opt out of ADMT due to good faith and documented belief that the request is fraudulent to inform the requestor that it will not comply and explain why it believes the request is fraudulent. (*See* § 7221(g), which is also consistent with existing requirements with respect to consumers' exercise of other existing CCPA rights in §§ 7026(e), 7027(f).)
7221(a)	830	Comment concerned that "opt-out" does not properly describe the issues that arise from ADMTs. Comment believes that a more detailed transparency schema is required. We advise the prior disclosure of consequences associated with the "opt-out" of an ADMT in regard to: 1. buying/selling/sharing/trading of personal information; 2. data retention of personal	The Agency disagrees with this comment. The regulations ensure that consumers have meaningful information about use the of ADMT with respect to them when they are exercising their CCPA rights. (*See* § 7220.) They also provide a flexible, performance-based standard for businesses regarding how to

		information; and 3. consequences and expected negative impacts to the consumer of the choice.	provide the required information. Additional disclosure requirements are not necessary.
7221(b)	93	Comment argues that workers should have the same rights as consumers to opt out of harmful or intrusive ADMTs. It emphasizes the importance of transparency and human oversight, especially for decisions affecting employment and privacy.	The Agency agrees with this comment. With respect to comment's statement that workers should have the same rights as consumers, the CCPA specifically includes employees and independent contractors within its scope. Article 11 provides these workers with the ability to opt-out of the use of ADMT to make a significant decision about them, which includes employment decisions. With respect to transparency, the regulations provide it via the Pre-use Notice and access ADMT requirements. With respect to human oversight, businesses must conduct a risk assessment prior to using ADMT to make a significant decision and for certain automated processing in the workplace. In addition, business can provide consumers with the ability to appeal a significant decision to a human reviewer instead of providing an opt-out.
7221(b)	94, 1084, 1086	Comment criticizes that the regulations introduce complex exceptions that undermine worker protections, making it easier for employers to evade accountability. Comment argues that the regulations contain broad exceptions that weaken workers' ability to opt out of algorithmic systems that may track, evaluate, or discriminate against them, undermining an essential right. The proposed regulations should apply broadly to all employment-related uses of AI, not just those an employer claims "substantially facilitate" decision-making.	The Agency disagrees with this comment. The exceptions to the opt-out right do not make it easy to evade accountability. The regulations are clear about what a business must do to qualify for an exception, and are necessary to address scenarios where, for example, it may not be feasible to provide consumers with an opt-out. In addition, § 7221 has been revised to simplify and clarify these exceptions. These revised exceptions also provide protections for consumers if they cannot opt-out, such as via human appeal or protections against unlawful discrimination.
7221(b)	99	Comment recommends shortening the appeal timelines for "highly consequential ADMT decisions." The regulations allow businesses 45 to 90 days to process ADMT appeals, which is too long for workers facing	The Agency disagrees with this comment. The timeline for the human appeal process is intended to be consistent with timelines for businesses' responses to consumers for other CCPA requests, which

		urgent economic consequences, such as job loss. Comment recommends 14 calendar days for responses.	balances burdens on businesses to come into compliance with ensuring consumers receive a response in a reasonable timeframe.
7221(b)	188, 288, 587, 880, 1564, 1764	Comment suggests the Agency should consider more appropriately scoping the other exemptions in its ADMT rule: "For admission, acceptance, or hiring decisions as set forth in § 7200, subsections (a)(1)(A)(i), (a)(1)(B)(i), if the following are true: (A) The automated decisionmaking technology is for the business's assessment of the consumer's ability to perform at work or in an educational program to determine whether to admit, accept, or hire them[.]" Corresponding revisions should be made to §§ 7221(b)(4) and (b)(5). Comment also states that these provisions impose significant challenges for companies attempting to use the employee-related exceptions to ADMT opt-out requirements. These sections require businesses to conduct evaluations and implement costly safeguards, which create unnecessary barriers for employers managing productivity and staffing needs. Additionally, terms like "work or educational profiling" lack clear definitions, causing further ambiguity, as the proposed regulations instead refer to "extensive profiling." Alternatively, comment suggests that "necessary to achieve" should be struck from or revised in 7221(b)(1), (3)(A), (4)(A), and (5)(A). Comment suggests that the exemptions in § 7721(b) should be clarified to align with the statutory exemption for the deletion right. The § 7221(b) standard could otherwise prevent ADMT from being used in cases where it is the best or most efficient method, even if alternatives exist. This could weaken fraud prevention and security efforts. Additionally, the security and fraud exception to the opt-out requirement contained in § 7221(b)(1) should apply to all uses of	The Agency disagrees with this comment. The Agency revised Article 11 to focus on the use of ADMT for significant decisions to simplify implementation at this time. The Agency has accordingly revised the exceptions to when a business must provide an opt-out from its use of ADMT, including removing the security, fraud prevention, and safety exception because it is unnecessary. These revisions also include removing references to "work or educational profiling" from § 7221. With respect to the exception for admissions, acceptance and hiring decisions in § 7221(b)(2), previously § 7221(b)(3)(A), and the exception for allocation/assignment of work and compensation decisions in § 7221(b)(3), previously § 7221(b)(4)(A), the Agency has removed the requirement that the ADMT be "necessary to achieve" the purposes set forth in those subsections, to simplify implementation for businesses at this time. However, the Agency has retained the requirement in §§ 7221(b)(2) and (b)(3), previously §§ 7221(b)(3) and (b)(4), that the ADMT be used "solely for" the purpose, to ensure exceptions to the right to opt-out of ADMT are not overly broad. The Agency has also revised the regulations to include a performance-based standard that the ADMT work for the business's purpose and does not unlawfully discriminate based upon protected characteristics. This balances protections for consumer privacy and simplifying implementation for businesses at this time. With respect to the comment's suggestion that the exceptions should be expanded to allow for improving and enhancing

		ADMT set forth in § 7200(a). Further, the Agency should expand these exceptions to allow for the use of ADMTs to improve and enhance these systems.	systems, the suggestion is less effective than the regulations at protecting consumer privacy, because it would limit consumers' ability to exercise their opt-out of ADMT right.
7221(b)	286	Comment recommends expanding the list of exceptions in this provision to include other back-end tasks such as conducting internal research, fixing technical errors, executing product recalls, and performing internal operations consistent with consumer expectations. Doing so would increase business's quality of service without degrading consumer privacy.	The Agency disagrees with this comment. Adding exceptions to consumers' right to opt out of ADMT would limit their right, which would be inconsistent with the purpose and intent of the CCPA. In addition, the Agency revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time.
7221(b)	287, 882, 934, 1562	Comment suggests that the terms "necessary to achieve" must be removed from §§ 7221(b)(1), (3)(A), (4)(A), and (5)(A). Comment believes that the "necessary to achieve" standard in § 7221(b) is too restrictive and could unintentionally prohibit beneficial uses of ADMT, such as fraud prevention and work performance assessments. The requirement should be removed while keeping the exceptions intact. Businesses should be free to choose the most effective and reasonable method of security, fraud prevention, or safety without regard for whether a particular method is "necessary." Comment recommends exchanging "is necessary" to "solely" and delete "and is used solely for."	The Agency disagrees with this comment. The Agency deleted the security, fraud prevention, and safety exception in previous § 7221(b)(1) because it is no longer necessary. With respect to the remaining opt-out exceptions in §§ 7221(b)(2) and (3), previously §§ 7221(b)(3) and (4), the Agency has removed the requirement that the ADMT be "necessary to achieve" the purposes set forth in those subsections, to simplify implementation for businesses at this time. However, the Agency has retained the requirement that the ADMT be used "solely for" the purpose, to ensure exceptions to the right to opt-out of ADMT are not overly broad. This balances protections for consumer privacy and simplifying implementation for businesses at this time.
7221(b)	442	Comment supports provisions for contestability in automated decisions, advocating that consumers must be provided with an appeal process to challenge significant decisions made by ADMT. This process should involve a qualified human reviewer with the	The Agency agrees in part with this comment, to the extent it supports the human appeal exception's requirements in § 7221. The Agency does not believe that additional requirements are not necessary at this time. The regulations balance providing safeguards

		authority to overturn decisions, and businesses should clearly explain how consumers can submit appeals.	for consumers for the human appeal exception with the burden on businesses to qualify for this exception.
7221(b)	1000, 1501	Comment raises concerns that § 7221(b) improperly limits opt-out rights for certain ADMT uses, such as uses related to education and work. They recommend striking certain subsections to ensure broader opt-out rights. Alternatively, these exceptions need to be further clarified and narrowed to properly protect people's rights.	The Agency disagrees with this comment. The exceptions address circumstances where an opt-out may not be feasible and provide businesses with flexibility regarding how to address consumers' concerns about the use of ADMT to make significant decisions about them. They also balance protections for consumer privacy and simplifying implementation for businesses at this time.
7221(b)	1495	Comment recommends amending § 7221(b) to state that affected businesses do not have to provide opt-out rights if personal information is aggregated and de-identified once it is provided for automated decisionmaking. If such information cannot be reasonably associated or linked, directly or indirectly, with a particular consumer or household, it should qualify as an exception to the opt-out requirement.	The Agency disagrees with this comment. The CCPA is reasonably clear in addressing which data are subject to the CCPA. (*See* Civ. Code § 1798.140(v)(3), stating that "personal information" does not include consumer information that is deidentified or aggregate consumer information.") All of the CCPA's exemptions apply to the regulations, and the Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. To the extent a business is processing personal information, it is subject to the CCPA's requirements, including Article 11's requirements for uses of ADMT for a signification decision.
7221(b)	1683	The Agency should remove the human appeal exception to the right to opt out of ADMT use. This weakens the opt-out provision. A human appeal process should be required in addition to an opt-out provision. The current exception provides a path for businesses to avoid providing opt-outs by having human reviewers rubber-stamp ADMT outputs. Human reviewers are likely to be biased toward affirming the ADMT decision.	The Agency disagrees with this comment. The human appeal exception is necessary to provide flexibility to businesses regarding how to address consumers' concerns about the use of ADMT to make significant decisions about them. The human appeal exception also has clear requirements about what must be provided to the consumer and how the decision must be reviewed, which addresses comment's concerns about bias and rubber-stamping.

7221(b)	1610, 1845	Comment recommends the inclusion of a catch-all exception to § 7221 for circumstances in which a business can demonstrate a compelling justification for not providing opt-out rights — especially when the ADMT use does not present significant risk to consumers' privacy or security. Alternatively, comment suggests an exception for processing that is necessary to perform a service requested by the consumer. The "opt-out" requirements pose a serious obstacle to functionality, and the proposed exceptions in § 7221(b) are too narrow and contain requirements too disconnected from consumer privacy protection to fall under the Agency's mission or serve its purposes.	The Agency disagrees with this comment, because the uses of ADMT subject to Article 11's requirements are already limited to when the use of ADMT is for a significant decision. In addition, the comment's suggestion to add a catch-all or necessity exception would limit consumers' right to opt out of ADMT, which would be inconsistent with the purpose and intent of the CCPA. Expanding or modifying the exceptions are not necessary. The current opt-out framework balances protections for consumer privacy and simplifying implementation for businesses at this time.
7221(b)	1970	Comment asserts that the exceptions for security, fraud detection, and safety should be construed narrowly. Without these changes, the privacy protections may be easily side stepped or denied to consumers.	The Agency disagrees with this comment. The security, fraud prevention, and safety exception has been removed from § 7221(b) because it is no longer necessary. However, the Agency revised the regulations to expand security/fraud-prevention/safety exceptions elsewhere within the regulations, to cover malicious activities directed at consumers. (*See* §§ 7220(d)(2)(B), 7222(c)(2)(B), 7027(m)(3).)
Previous 7221(b)(1)	95	Comment suggests adding guardrails on the "security, fraud prevention, and safety exception" in § 7221 to prevent businesses from misusing it. Additionally, workers and consumers should receive a written explanation justifying the necessity of ADMT-based decisions. Businesses should also be required to provide specific details when alleging fraud or dishonesty, ensuring that individuals can challenge such claims effectively.	The Agency has removed the security, fraud prevention, and safety exception. This exception is no longer necessary due to the revised scope of Article 11.

DRAFT

7221(b)(1) [previously 7221(b)(2)]	97	Comment recommends strengthening the human review and appeal requirements under the "human appeal exception." The human appeal exception is currently too weak to ensure fair decision-making. Businesses are only required to provide a "qualified" human reviewer who has the "authority to overturn" ADMT decisions. Additional procedural improvements should require allocation of human resources for effective appeals; expressly provide protection from retaliation; provide additional protections related to training, impartiality, anti-bias, and conflict-of-interest; make appeals more accessible and deter arbitrary decisionmaking; ensure workers can be represented by advisors and receive clear written explanations for appeal outcomes; and require businesses undertake certain actions to prevent reoccurrence of erroneous decisions.	The Agency disagrees with this comment. The human appeal exception provides clear requirements for both the human reviewer and the process of the appeal, and has been revised to provide additional clarity about the qualifications of the human reviewer and what they must do. The Agency believes the exception's requirements are sufficient and appropriate at this time. They ensure that consumers can easily exercise the human appeal option, such as requiring that the method of appeal is easy to execute and require minimal steps. They provide protections for consumers, such as requiring that the human reviewer have the authority to change the decision and know how to interpret and use the output of the ADMT. They also provide a performance standard that give businesses flexibility to determine how to provide a human appeal mechanism that is appropriate to how they use ADMT.
7221(b)(1) [previously 7221(b)(2)]	98	Comment recommends requiring ex-ante human review and expedited appeals for "highly-consequential decisions" when claiming the human appeal exception. For high-impact decisions like hiring, firing, and compensation, human review should occur before an ADMT decision is finalized — not just afterward.	The Agency disagrees with this comment. The human appeal exception provides clear requirements for both the human reviewer and the process of the appeal, and has been revised to provide additional clarity about the qualifications of the human reviewer and what they must do. The Agency believes the exception's requirements are sufficient and appropriate at this time. They ensure that consumers can easily exercise the human appeal option, such as requiring that the method of appeal is easy to execute and require minimal steps. They provide protections for consumers, such as requiring that the human reviewer have the authority to change the decision and know how to interpret and use the output of the

			ADMT. They also provide a performance standard that give businesses flexibility to determine how to provide a human appeal mechanism that is appropriate to how they use ADMT.
7221(b)(1) [previously 7221(b)(2)]	412, 755	Comment argues that this provision attempts to include human intervention in opt-out rules for ADMT-based decisions. Instead, opt-out rights should align with GDPR's definition of "significant decisions" (i.e., those with legal or similarly significant effects). The inappropriately overbroad definition of "significant decision" should be revised to mirror the GDPR concept requiring both human intervention and a legal or similarly significant effect. The regulation should clarify that human intervention mitigates the need for opt-out rights, simplifying compliance.	The Agency disagrees with the comment. The definitions of ADMT and significant decision are clear and not overly broad. The Agency also revised the definitions to provide further clarity and simplify implementation for businesses at this time. Further, the Agency revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. The regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. Notwithstanding the Agency's revisions to the ADMT definition and the thresholds for when a business must comply with the ADMT requirements, the human-appeal exception provides both clarity and flexibility for businesses regarding how to address consumers' concerns about the use of ADMT to make significant decisions about them. Additional clarification is not necessary.
7221(b)(1) [previously 7221(b)(2)]	787	Comment claims that the proposed opt-out provisions for ADMT in the employment and hiring context could make certain business processes unworkable and costly. The supposed exception allowing appeals to a "qualified human reviewer" is essentially a requirement to opt out.	The Agency disagrees with the comment. The human appeal exception is distinct from the opt-out requirements. The opt-out requirements are not unworkable or unduly burdensome. Instead, they ensure consumers can meaningfully opt-out of the use of ADMT to make a significant decision while providing flexibility for businesses to come into compliance.

7221(b)(1) [previously 7221(b)(2)]	948	Comment argues that the proposed human appeal mechanism is unnecessary when ADMT is not the sole decision-maker. If human judgment is involved in a decision (e.g., an HR manager reviewing attendance data), an additional appeal right is redundant. The opt-out right should be limited to fully automated decisions.	The Agency disagrees with this comment. The human-appeal exception provides flexibility for businesses regarding how to address consumers' concerns about the use of ADMT to make significant decisions about them. Human appeal addresses circumstances where an opt-out may not be feasible to provide, but human appeal can be provided after a decision is made using ADMT.
7221(b)(1) [previously 7221(b)(2)]	971, 1502, 1753, 1968	Comment suggests that the "human appeal" exception under § 7221(b)(2) should be removed because research shows that human reviewers are likely to defer to algorithmic decisions, turning the appeal into a rubber-stamping exercise and undermining opt-out rights. Alternatively, comment urges revisions to § 7221(b)(2) and recommend a set of detailed procedural safeguards to ensure appeals are fair and reliable. Comment suggests that the human appeal process for ADMT decisions needs improvements to clarify what qualifies a reviewer, prevent conflicts of interest, protect reviewers from retaliation, and ensure companies properly fund the appeals process.	The Agency disagrees with this comment. Comment's suggested revisions are not more effective or appropriate than those proposed by the Agency. The regulations balance privacy protections for consumers and flexibility for businesses regarding how to address consumers' concerns about the use of ADMT to make significant decisions about them. The Agency also revised the human-appeal exception to clarify what a business must do to qualify for the human appeal exception. The exception includes requirements such as the human reviewer considering the information the consumer provided in support of their appeal, knowing how to interpret and use the output of the ADMT, and having the authority to change the significant decision based upon their analysis. Additional modifications are not necessary at this time.
7221(b)(2) [previously 7221(b)(3)]	788	Comment suggests that the exemption under § 7221(b)(3) is too narrow, as it only applies when ADMT is "necessary" and "used solely for" specific, undefined purposes. The comment suggests broadening the exemption to cover all employment-related decisions.	The Agency disagrees with this comment. However, the Agency has removed the requirement that the ADMT be "necessary to achieve" the purpose, to simplify implementation for businesses at this time. The Agency has retained the requirement that the ADMT be used solely assessing the consumer's ability to perform to determine whether to admit, accept, or hire them, to ensure the exceptions to the opt-out

			right are not overly broad. In addition, the regulations define "performance at work" and "performance in an educational program," which provide additional clarity for businesses. Comment's suggestion to cover all employment-related decisions is less effective than the regulations, because it would limit consumers' ability to opt out.
7221(b)(2)(A) [previously 7221(b)(3)(A)]	1504	Comment believes that the term "necessary" in the exceptions should be better defined to prevent businesses from justifying profit-motivated ADMT use under the guise of necessity. Examples from university admissions and warehouse employee surveillance show that many such systems are not truly necessary.	The Agency disagrees with this comment, to the extent it suggests that the regulation is not clear. In addition, the Agency has removed the requirements that the ADMT be "necessary to achieve" the purposes set forth in those subsections, to simplify implementation for businesses at this time.
7221(b)(2) [previously 7221(b)(3)], 7221(b)(3) [previously 7221(b)(4)], previous 7221(b)(5)	96	Comment recommends eliminating the overly broad "hiring," "allocation/assignment of work and compensation," and "work profiling" exceptions under §§ 7221(b)(3), (b)(4), and (b)(5). The current draft regulations contain vague and broad exceptions for ADMT use in key employment areas, such as hiring, work assignment, and compensation. These exceptions only require businesses to claim that ADMT use is "necessary" and do not have clear standards for evaluation.	The Agency disagrees in part with this comment. With respect to the hiring and allocation/assignment of work and compensation exceptions, these have been retained to address circumstances where it may not be feasible to provide consumers with an opt-out. These exceptions have also been revised to further clarify what a business must do to meet their provisions. With respect to the "work profiling" exception, this exception has been deleted because it is no longer necessary. That exception's corresponding "work threshold" in § 7200(a) has been deleted.
Previous 7221(b)(5)(B)(i)	835	Comment does not recommend upholding the exclusions for work or educational profiling, because most providers of ADMT insufficiently engage in bias mitigation themselves and have questionable casual hypothesis and construct validity. They also do not provide validation mechanisms from the consumer to validate the inferential personal data. These tools raise valid questions of workplace intrusion that are not	The Agency disagrees with this comment. The Agency revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. The Agency has accordingly removed references to work/educational profiling from § 7221, and the corresponding opt-out exception. To the extent that the comment suggests that the Agency should impose additional requirements regarding

		justified by safety or security concerns. Employees, contractors, and gig-workers are effectively vulnerable populations by the nature of their largely powerless position. Failure to strike these exclusions should result in robust protocols required to uphold antidiscrimination, unfair, deceptive, and abusive practices, and data privacy laws such as transparency of what is tracked, the ability to validate the data captured, and assessments of fairness conducted by a trained ethics committee.	discrimination; unfair deceptive, or abusive practices; transparency; validation; and fairness, the Agency has not included such requirements to simplify implementation of these regulations at this time. The Agency will monitor the need for additional protections for consumers' privacy as businesses come into compliance with these regulations.
Previous 7221(b)(6)	189, 876, 935	Comment suggests that the regulations should not require opt-out rights for training ADMT and behavioral advertising, as this could increase AI bias and disrupt first-party personalization efforts. Instead, opt-out rights should be limited to "cross-context behavioral advertising" under Civil Code § 1798.140(k). Comment suggests deletion of this provision or revising as follows: "The exceptions in this subsection do not apply to profiling for behavioral advertising as set forth in section 7200, subsection (a)(2)(C). A business must provide the ability to opt-out of these uses of automated decisionmaking technology in all circumstances."	The Agency disagrees with this comment. However, the Agency has revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. This includes removing the profiling for behavioral advertising and training ADMT thresholds from the ADMT regulations.
Previous 7221(b)(6)	836	Comment affirms that there are no applicable exclusions for behavioral advertising.	The Agency has revised the regulations to remove the profiling for behavioral advertising threshold, to simplify implementation for businesses at this time.
7221(c)	936	Comment suggests that the requirement in § 7221(c) to provide two opt-out methods is excessive and should be reduced to one method for efficiency and consistency.	The Agency disagrees with this comment. The requirement balances consumers receiving meaningful access to their right to opt-out of ADMT and flexibility for businesses in determining how to receive opt-out of ADMT requests. It is also consistent with similar requirements for other CCPA rights. (*See* §§ 7026(a), 7027(b).) This enables businesses to leverage their existing CCPA opt-out methods and

			extend them to the right to opt-out of ADMT, while ensuring that at least one of the methods for submitting requests reflects the manner in which the consumer interacts with the business.
7221(c)(1)	950, 1463	Comment argues that requiring businesses to provide both a "Do Not Sell/Share" link and an "Opt-out of Automated Decisionmaking Technology" link will confuse consumers and create unnecessary compliance burdens. A streamlined approach should allow businesses that offer a CCBA opt-out to rely on that mechanism for ADMT opt-outs. Comment recommends adding a subsection stating that in lieu of posting an opt-out link, a business may include the opt-out on the webpage of the alterative opt-out link in accordance with § 7015.	The Agency disagrees with this comment. The Agency has revised § 7221(c)(1) to remove the requirement that the link be titled "Opt-out of Automated Decisionmaking Technology" and instead require that the link state what the consumer is opting out of, with "Opt-out of Automated Decisionmaking Technology" being an example. This revision simplifies implementation for businesses at this time and provides them with more flexibility. The comment's suggestion also implies that businesses would not need to provide an opt-out link in the Pre-use Notice, which would weaken consumers' ability to exercise their opt-out right. Businesses have flexibility to include an opt-out link in other places, but must include it in the Pre-use Notice.
7221(c)(4)	1462	Comment suggests deleting the subsection explaining that a notification or tool regarding cookies is not by itself an acceptable method for submitting requests to opt-out of ADMT.	The Agency disagrees with this comment because the subsection is necessary to ensure that consumers are aware of and can easily exercise their right to opt-out of ADMT. The Agency determined this explanation necessary based on its observations in the marketplace of businesses inappropriately using cookie banners or controls. The regulation also ensures that businesses do not choose obscure methods for consumers to submit requests. It also promotes consistency in how consumers can exercise their CCPA opt-out rights under existing regulations. (*See* §§ 7026(a)(1)–(4), 7027(b)(1)–(4).)

DRAFT

7221(g)	190, 413, 756	Comment suggests that this provision could unintentionally assist fraudsters by revealing detection methods and recommends removing this provision to protect businesses from fraud-related risks. Comment suggests the Agency revise this provision to avoid forcing businesses to provide information to bad actors that they can use to further fraudulent activities: "If a business has a good-faith, reasonable, and documented belief that a request to opt-out of ADMT is fraudulent, the business may deny the request. The business must inform the requestor that it will not comply with the request."	The Agency disagrees with this comment. The requirement imposes a minimal burden on businesses while protecting consumers' right to opt-out of ADMT, consistent with the purpose and intent of the CCPA. The requirement ensures that consumers' legitimate requests are not denied as potentially fraudulent without explanation and is consistent with existing requirements of businesses and protections for consumers' existing CCPA rights. (*See* §§ 7026(e), 7027(f).) This enables businesses to leverage existing processes for other CCPA rights and extend them to the right to opt-out of ADMT. The comment also does not explain, and the Agency does not agree, that providing an explanation would harm security, especially given that the regulations do not require businesses to reveal their detection methods; businesses have discretion in crafting the explanation.
7221(h)	1939	Comment suggests revising the regulation to state that a clear notification be given that the consumer has successfully opted-out. Comments suggests the text "you've been opted out" or similar. It prevents all the UI games sites are playing now where it is impossible to tell if one has opted out or not.	The Agency disagrees with this comment. The regulations already include a requirement that a business provide a means by which the consumer can confirm that the business has processed their request to opt-out of ADMT. The comment's suggestion is not more effective or appropriate than those adopted by the Agency.
7221(i)	289, 1113, 1114, 1357, 1563, 1639, 1771	Comment states that the regulations would force businesses to offer a single opt-out for all covered ADMT, although businesses may let consumers allow specific uses. Businesses should instead be required to offer opt-outs targeting the specific use cases applicable to a consumer's data. Requiring context-specific opt-outs will give consumers more autonomy and insight regarding the use of their data. This approach aligns with existing CCPA deletion	The Agency disagrees with this comment. Requiring a business to provide a single option to opt-out of all covered ADMT is necessary to prevent consumer confusion and to prevent businesses from presenting options to consumers in a strategic manner intended to curtail exercise of their right. It is also consistent with similar existing requirements for other CCPA rights (*see* §§ 7026(h), 7027(i)), which benefits businesses by enabling them to leverage existing

		regulations, which permit a business to present a consumer with the choice to delete select portions of their personal information. A single opt-out choice for ADMT incorrectly presumes that all ADMT uses subject to the regulations lack benefits to consumers, and is antithetical to California's support for innovation, efficiency, and tools that reduce human error and bias. Furthermore, the single opt-out structure does not advance the interests of California consumers, who might want to opt out of some, but not all, uses of ADMT. Comment states that requiring a single opt-out option for all ADMT use cases does not consider the nuances between different applications. This approach could lead consumers to opt out broadly without understanding potential benefits. Instead, business should be required to surface an opt out that is targeted to the specific use case so the consumer can decide in real time and in context rather than in the abstract. Comment recommends amending § 7221(i) as follows: In responding to a request to opt-out of ADMT, a business may present the consumer with the choice to allow specific uses of automated decisionmaking technology. The opt-out requirement also could negatively impact grocery retailers' rewards and loyalty programs, which rely on ADMT to personalize customer experiences. Independent grocers use these programs to compete with larger stores, and restricting ADMT could harm their ability to offer incentives. The proposed rules may also unintentionally apply to contextual advertising, which does not involve tracking over time, creating unintended restrictions. If an exclusion is not granted, the opt-out should at least align with California's existing statutory opt-out framework, which is limited to cross-context behavioral advertising.	processes for other CCPA rights and extend them to the opt-out of ADMT. The requirement does not prohibit a business from providing context-specific opt-out of ADMT information, as long as the business also offers a single option to opt out of all covered ADMT. With respect to the opt-out requirement for profiling for behavioral advertising, the regulations are within the Agency's authority and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(15).) The definition of behavioral advertising excluded non-personalized advertising (*see* § 7001(g)(2).) However, the Agency has revised the regulations to remove profiling for behavioral advertising, to simplify implementation for businesses at this time.

7221(j)	592	Comment suggests allowing authorized agents to submit ADMT opt-out requests with a signed written permission presents security and operational risks. Thus, the Agency should remove agent-based opt-outs from ADMT-related provisions.	The Agency disagrees with this comment. Not permitting consumers to use authorized agents to facilitate opt-out of ADMT requests would limit this right, which would be inconsistent with the purpose and intent of the CCPA. The regulations include protections for consumers' use of authorized agents, including requiring a consumer to have provided signed permission to the agent, and allowing a business to deny an authorized agent's request if the agent does not provide the signed permission to the business. Permitting consumers to use authorized agents with these safeguards is also consistent with other CCPA rights, which enables businesses to leverage their existing processes for CCPA rights and extend them to the right to opt-out of ADMT. (*See* §§ 7026(j), 7027(j).)
7221(j)	1940	Suggests adding "which may be evidenced via electronic signature" in this subsection. Comment states that it is important to remove barriers especially since this is an opt-out and does not result in a consumer's information being disclosed. Also, it's possible to do so much now via the electronic binding agreement services. The Agency should be encouraging ease of exercising consumer rights.	The Agency disagrees with this comment, because it is unnecessary. The regulations already provide for the validity of electronic signatures. (*See* § 7001(ii).)
7221(*l*)	100, 972	Comment recommends expressly prohibiting businesses from retaliating against consumers who have exercised their access and appeal rights. Comment points out that consumers must be explicitly protected from retaliation when exercising ADMT-related rights, such as opting out, appealing a decision, or accessing ADMT information.	The Agency disagrees with this comment, to the extent it suggests that the CCPA does not prohibit retaliation. The CCPA already prohibits businesses from retaliating against consumers for exercising their CCPA rights. (*See* Civ. Code § 1798.125(a)(1).)

7221(*l*)	1770	Comment argues that the draft rules do not clarify what happens when consumers opt out of ADMT but the business has no other means to provide the service. Businesses may unintentionally violate § 7221(*l*) if they are unable to serve these consumers. The Agency should reconsider, or clarify, the operational impact of these processes, and should clarify that businesses using covered ADMT are not required to provide their services by other means, if doing so would be technically infeasible.	The Agency disagrees with this comment. The opt-out exceptions already address circumstances where an opt-out of ADMT may not be feasible. Additional exceptions or clarifications are not necessary.
7221(m), 7221(n)	185	Comment suggests the revision of §§ 7221(m) and (n), including deletion of § 7221(n)(2). § 7221(m): "If the consumer submits a request to opt-out of ADMT before the business has initiated that processing, the business must not initiate processing of the consumer's personal information for the purposes set forth in § 7200, subsection (a) using that automated decisionmaking technology." § 7221(n): "If the consumer did not opt-out in response to the Pre-use Notice, and submitted a request to opt-out of ADMT after the business initiated the processing, the business must comply with the consumer's opt-out request by: (1) Ceasing to process the consumer's personal information for the purposes set forth in § 7200, subsection (a) using that automated decisionmaking technology as soon as feasibly possible, but no later than 15 business days from the date the business receives the request."	The Agency disagrees with the comment. The suggested revision to § 7221(m) is unnecessary. The regulations only require a business to provide an opt-out from its use of ADMT when a business uses ADMT as set forth in § 7200(a). It is unnecessary for § 7221(m) to restate those uses. In addition, the Agency has revised § 7221(n)(1) 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." This is already addressed by the first sentence of subsection (n)(1). The Agency also disagrees with the comment's suggested deletion of § 7221(n)(2) requiring businesses to notify other persons to whom the business has made the consumer's personal information available using that ADMT that the consumer has opted out. Instructing them to comply with the consumer's opt-out is necessary to protect consumers' right to opt-out of ADMT. This requirement is also consistent with other CCPA opt-out rights. (*See* §§ 7022, 7026(f), 7027(g).)

7221(n)	590, 674, 1723, 1899, 1859, 1953	Comment suggests removing the backward facing element of ADMT opt-outs in 7221(n). Comment states that requiring businesses to remove previously collected data from ADMT models is impractical and could conflict with de-identification principles and is technically unworkable. Comment argues that this requirement would also be massively expensive and burdensome. Comment expresses concern that it would be technically and practically challenging to retrain AI models initially trained on personal information that are later subject to an opt-out request, and that the Agency must further clarify this provision. Comment requests to clarify that the opt-out should only apply prospectively, like other CCPA rights. Comment highlights that AI models typically rely on de-identified data which cannot easily be attributed back to an individual or reasonably permit reidentification. Retroactive deletion could harm service quality for consumers. Comment recommends that the Agency should omit the potentially backward-looking component of the ADMT opt out by amending §§ 7221(m)-(n). Comment believes that the requirement in § 7221(n) to cease processing and neither use nor retain previously processed information could also compromise important HR record-keeping needs and compliance obligations. Comment suggests clarifying that requests to opt-out of ADMT after the business has initiated processing do not require retraining of models under § 7221(n).	The Agency disagrees with this comment. The deletion requirement is neither impractical nor unworkable. The Agency has also revised § 7221(n)(1) 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." This is already addressed by the first sentence of subsection (n)(1). In addition, the Agency has revised § 7200 to focus on the use of ADMT for significant decisions to simplify implementation at this time. This includes removing the training threshold from Article 11.
7221(o)	1378	Comment suggests revisions to this section by adding "prior to the commencement of processing," stating "[c]easing to engage in such ADMT in connection with such consumer using the consumer's personal	The Agency disagrees with this comment. The regulation is clear that a business must not process the consumer's personal information using the ADMT that the consumer has opted out of. The comment's revisions are less clear than the regulation and would

		information" in subsection (o)(1), and deleting the last sentence of § 7221(o)(1).	be more difficult for businesses to comply with. The Agency also deleted the second sentence in § 7221(n)(1), previously § 7221(o)(1), regarding the prohibition on using or retaining that information because is already addressed in the first sentence.
7222	92, 782, 974	Comment recommends clarifying that consumers can use authorized agents for access ADMT requests. Comment states that workers can then designate authorized representatives, such as unions or worker organizations, to access information about ADMT decisions on their behalf. This would help workers who may lack the resources or expertise to navigate data access requests. Concerns about abuse by paid agents are unfounded and should not limit this protection.	The Agency disagrees with this comment. The Agency has not included this provision to simplify implementation of these regulations at this time. The Agency will monitor the need for such access options as businesses come into compliance with these regulations.
7222	217, 290, 292, 367, 537, 594, 595, 676, 677, 682, 757, 758, 860, 877, 938, 960, 1193, 1194, 1342, 1343, 1361, 1567, 1569, 1642, 1644, 1724, 1842,	Comment claims that the proposed regulations under § 7222 exceed the authority granted by the CCPA. Civil Code § 1798.185 only requires businesses to provide "meaningful information about the logic involved" in ADMT and a "description of the likely outcome." However, § 7222 imposes obligations that go beyond this, including consumer-specific disclosures and additional notice requirements that create unnecessary compliance burdens and could expose proprietary information. Additionally, the disclosure of information related to the outputs generated by ADMT and how those outputs influence decisions conflicts with other statutory exemptions, such as the recognition that the statute does not require a business to process personal information that would limit the business's ability to exercise or defend legal claims or comply with the law. § 7222(b) is also overly broad, burdensome, and costly, and raises data retention and governance challenges. Further, the requirement to provide consumers with	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, it is required to issue regulations and impose certain requirements on these topics. Moreover, the Agency engaged in robust preliminary rulemaking activities with a wide variety of stakeholders, has collaborated with state lawmakers and will continue to do so. (*See* Civ. Code § 1798.199.40(g).) With respect to notices to consumers, the notice requirements in the regulations provide businesses with flexibility in how they are consolidated or provided to consumers. The Agency disagrees that the notice requirements would impede consumers, because these notices ensure that

	1850, 1901	information about other actions they could have taken to secure a different decision is far too prescriptive and not aligned with existing law, which already provides consumers with rights to substantial information. Comment also states that individual responses are often impractical, infeasible, and risk exposing proprietary information or trade secrets in conflict with Civil Code 1798.185(a)(3), which protects proprietary business information. Requiring disclosures could also expose confidential business processes and facilitate gaming of systems like university admissions. Comment suggests that requiring the disclosure of detailed parameters that affect ADMT outputs is overly intrusive, could harm consumer trust and business operations and enable malicious and deceptive activity, reveal sensitive business information, and be difficult to ascertain with respect to a particular decision. Comment also claims that the requirement to disclose ADMT logic in "plain language" is impractical because advanced AI models are too complex to explain concisely without being misleading. Further, prescriptive explainability requirements ignore disclosures of what is possible regarding explainability. Technologists continue to research and do not agree on whether and to what extent ADMT decisions can be provided in a way that offers "meaningful information" to consumers. Comment makes several suggestions. This includes deleting these requirements or streamlining them into a single rule allowing disclosure via general notices rather than consumer-specific responses. Comment also suggests modeling after language in existing law, such as MN's privacy law, or waiting for research to be further developed before imposing legal obligations that may be impractical based on the current state of	consumers have meaningful information prior to exercising their CCPA rights. The CCPA also explicitly requires that a business's response to access requests includes meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process, with respect to the consumer. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. A generalized notice would not meet the requirements of the CCPA. Further, consumer-specific and plain language requirements are not impractical or infeasible. Nevertheless, the Agency has revised the regulations to provide further clarity about what type of information may be provided to a consumer to meet the CCPA's requirements and to simplify implementation for businesses at this time. Moreover, the Agency also specifically exempts the disclosure of trade secrets and certain information related to security, fraud prevention, or safety from inclusion in the Pre-use Notice and the information provided to consumers in response to a request to access ADMT. (*See* §§ 7220(d), 7222(c).) The CCPA's statutory exemptions also apply to the regulations. The Agency does not believe additional exemptions are necessary at this time. With respect to retention, the CCPA states that it does not require a business to retain any personal information about a consumer if, in the ordinary course of business, that information about the consumer would not be retained. (Civ. Code § 1798.145(j).) In addition, the same retention obligations apply to the right to access ADMT as with other CCPA rights, as set forth in § 7101. This promotes consistency for recordkeeping for CCPA requests.

		science. Additional recommendations including permitting businesses to provide general potential outcomes rather than case-specific ones in § 7222(b)(2), and clarifying that businesses may describe ADMT's general functionality rather than its specific effect on each consumer in § 7222(b)(4). Comment also states that the proposed regulations should clarify that companies are not obligated to disclose trade secrets, proprietary designs, or confidential information about ADMT systems. The regulations should also extend the exemption for commercial credit data to ADMT access provisions, as ADMT access requirements in the commercial credit context do not provide meaningful information to individual consumers. Comment also suggests removing the requirement in § 7222(b) to provide an individualized explanation of how ADMT "worked with respect to the consumer" including the logic and parameters, output, and how the business used it. This requirement creates unnecessary compliance costs and may not provide meaningful insights to consumers. Comment suggests modifying § 7222(b)(2) so that the business must provide only the range of potential outputs and not the specific output as it relates to the consumer. If the output itself contains personal information related to the consumer, then it would be subject to the separate, broader access right under the CPRA. Comment also suggests that the Agency permit more flexibility in how businesses respond to access requests; remove any requirement to provide access to the logic or outcome of ADMT when ADMT is used only for fraud or security purposes or other purposes that are subject to exemptions under the CCPA; and remove the suggestion that businesses must provide special access concerning ADMT when	With respect to flexibility, the regulations explicitly allow a business to provide aggregate-level response if it used an ADMT with respect to a consumer more than four times within a 12-month period. This provides businesses with the flexibility to consolidate responses to access ADMT requests while still providing consumers with the ability to access ADMT. With respect to § 7222(k), the Agency disagrees that this requirement is burdensome and unnecessary but has removed the notice requirements for "adverse significant decisions" to simplify implementation for businesses at this time. Additionally, § 7222(h) clarifies the requirements of a service provider or contractor for requests to access ADMT; § 7222(i) provides a businesses with flexibility to consolidate responses to access ADMT; and § 7222(j) clarifies all the requirements for the right to access ADMT in one place and facilitates compliance with the prohibition against retaliation in the CCPA. The sections are not overly burdensome and the Agency has made efforts to limit the burden of the regulations while implementing the CCPA.

		humans are involved in the decisionmaking or where ADMT is used other than for significant decisions. Comment also states that mandatory notices for adverse significant decisions (§ 7222(k)) are burdensome and unnecessary. Comment also recommends deleting §§ 7222(h)-(j) as unnecessary.	
7222	600	Comment argues that an unlimited right for a consumer request to access ADMT creates a major data retention issue and conflicts with industry best practices with data minimization, which is a foundational principle in the CCPA. As currently drafted, a company must retain information related to all significant decisions indefinitely. This requirement is unreasonable and must be limited, either by limiting how long a consumer can request the information or how long a business must retain the information.	The Agency disagrees with this comment. The CCPA states that it does not require a business to retain any personal information about a consumer if, in the ordinary course of business, that information about the consumer would not be retained. (Civ. Code § 1798.145(j).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. With respect to consumer requests, the regulations explicitly allow a business to provide aggregate-level response if it used an ADMT with respect to a consumer more than four times within a 12-month period. This provides businesses with the flexibility to consolidate responses to access ADMT requests while still providing consumers with the ability to access ADMT.
7222	1195, 1229	Comment states that the access requirements could enable identity theft and fraud. Attackers who obtain stolen login credentials may exploit disclosure rules to gather sensitive consumer data for targeted scams. Similar issues have been identified with right-of-access requests under other privacy laws.	The Agency disagrees with this comment. When providing the required information for an access ADMT request, a business is not required to include certain security, fraud prevention, or safety information, as set forth in § 7222(c). These balance protections against identity theft and fraud with ensuring consumers receive meaningful information in response to an access ADMT request.
7222	1398	The regulations seek to regulate areas that are preempted by federal law. The Supremacy Clause of the U.S. Constitution prohibits states from regulating conduct "in a field that Congress, acting within its	The Agency disagrees with this comment. The regulations do not conflict with federal law. In addition, § 7222(c) of the revised regulations state that a business is not required to include trade secrets

		proper authority, has determined must be regulated by its exclusive governance." State laws are also preempted when they conflict with federal law, including when they stand "as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." Federal law protects trade secrets under the Defend Trade Secrets Act ("DTSA"), including "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes" that are kept "secret" and have "independent economic value . . . from not being generally known." While the DTSA does not "preempt or displace any other remedies provided by United States Federal [or] State . . . law for the misappropriation of a trade secret," California may not entirely abrogate the protections granted to a business's trade secrets. The regulations ignore the express trade secret exemption in the CCPA. For example, § 7222 requires a business to share commercially sensitive information with consumers, including the logic, assumptions, limitations, and key parameters of ADMT. Depending on the technology and business in question, and the level of detail expected by regulators, this information could constitute a business's trade secrets, required disclosure of which is preempted by federal law.	when providing the information required in § 7222(b)(2)-(3).
7222	1496	Comment suggests amending § 7222 to limit the right to access ADMT to accessing personally identifiable information only. If the information is not stored by the affected business in a manner that can be reasonably associated or linked, directly or indirectly, with a particular consumer or household, it should not be	The Agency disagrees with this comment. The CCPA provides statutory exemptions for certain information. The Agency cannot amend the CCP or adopt regulations inconsistent with the CCPA. The regulations also clarify that a business is not required to disclose trade secrets or certain security, fraud

		subject to an access request. This is consistent with the right to access information in California Civil Code § 1798.110, as well as general exceptions under § 1798.145(j)(1) and (j)(3).	prevention, or safety information. The Agency does not believe that additional exemptions are not necessary at this time.
7222	1612	Comment contends that the CCPA intends for consumers to have meaningful access rights regarding ADMT logic, as stated in the CCPA. However, the regulations currently require overly detailed disclosures that may exceed Agency's authority and risk exposing trade secrets and intellectual property.	The Agency agrees with this comment in part to the extent it indicates that the CCPA intends for consumers to have access rights to ADMT logic. The Agency otherwise disagrees with this comment. The ADMT regulations are within the Agency's authority and further the intent and purposes of the CCPA. The CCPA requires that businesses' response to access requests to include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process with respect to the consumer. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The regulations have been revised to provide additional clarity on how to provide the relevant information to consumers. The regulations also do not require businesses to disclose trade secrets when providing the required information in response to an access ADMT request.
7222	1909	Comment urges the Agency to either adopt an opt-in consent scheme for the use of ADMTs to process consumer information, or strengthen the opt-out right to allow consumers to prevent any of their sensitive information from being ingested into an algorithm. The current proposed Rule only provides a qualified right to opt out of ADMT processing with exemptions. The extensive exceptions compromise choice and thereby run afoul of the stated purpose of Article 11. Regardless of whether consumers opt in or out to exercise their ADMT rights, those rights should be more precisely and	The Agency disagrees with this comment. With respect to the opt-in, the CCPA requires that the Agency issue regulations governing access and opt-out rights with respect to a business's use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) Article 11 implements the statutory delegation. With respect to sensitive information, consumers already have a right to limit the use and disclosure of sensitive personal information under the CCPA, so the comment's recommendation is not necessary. With respect to the ADMT requirements, the regulations are clear

		comprehensively defined. In particular, the Rule should allow consumers to opt out of both having ADMTs used to make decisions about them and having their personal information used to train ADMTs.	regarding a business's obligation. Further, the Agency has revised the regulations to focus on the use of ADMT to make a significant decision to further simplify implementation for businesses at this time.
7222(a)	291, 1568, 1643	Comment argues that the rights in this section should apply only when ADMT is used to make a significant decision. Otherwise, it could require disclosure of confidential tech processes without meaningful benefit. Comment also argues that the access right lets consumers determine whether they want to exercise their opt-out right and correct any errors regarding their personal information. For other ADMT uses, such as profiling for behavioral advertising, consumers can choose to opt out regardless of how the technology works. Businesses should not need to publicly disclose confidential and/or proprietary information about their technology without any direct consumer benefit. Comment suggests amending § 7222(a) as follows:" Consumers have a right to access ADMT when a business uses automated decision-making technology as set forth in § 7200, subsections (a)(1)-(2)," and striking § 7222(b)(3)(B).	The Agency disagrees with this comment. However, the Agency has revised the regulations to focus on significant decisions to simplify implementation for businesses at this time. Additionally, businesses are not required to disclose trade secrets when providing the information required for requests to access ADMT.
Previous 7222(a)(1)	837	Comment finds this exclusion a direct violation of our human rights in regard to personal data. Future-looking approaches must require the following: 1. Robust chain-of-custody of data, 2. Differentiation of Inferential Personal Information and Factual Personal Information, 3. The Right to Correct factual errors, regardless of where they reside, as currently recognized already within the CCPA as to Personal Information; and 4. The Right to Delete Personal Data, also as currently recognized within the CCPA, balanced against right of the data processor and subject to data retentions laws,	The Agency disagrees with this comment. The exemption for training uses of ADMT was intended to limit the burden on businesses. Comment also acknowledges that the CCPA also provides consumers with rights to correct and delete their personal information. It is also unclear what the comment's recommendation is to ensure robust chain-of-custody of data or differentiation of inferential personal information and factual personal information. The CCPA does include a right to know, which includes inferences about a consumer and may address

		and public disclosure exclusions Organizations have a right to track data; they do not have a right to represent an unvalidated description of who a Consumer is, despite it being rampant in the industry today.	comment's concerns about inferential personal information. Lastly, the Agency has revised the regulation to remove the references to training uses of ADMT, and focus on the use of ADMT for significant decisions, to simplify implementation for businesses at this time.
Previous 7222(b)(3)(B)	838	Comment strongly recommends striking the word "extensive," as this subsection should apply to all forms of profiling, or, at the very least, profiling in furtherance of decisions that will have a significant legal impact. This is a critical provision of the AMDT regulations and it should not be limited to a small subset of profiling.	The Agency disagrees with this comment. The Agency has revised the regulations to focus on significant decisions, to simplify implementation for businesses at this time.
Previous 7222(b)(4)	91, 1507, 1754	Comment recommends reinstating the requirement that allows a worker to access aggregate outputs relevant to the use of an ADMT with respect to the worker. Transparency should extend to providing workers with aggregate comparison data to help them understand how ADMTs operate and how their individual data is assessed in relation to others. Comment also argues that post-use disclosures under § 7222(b)(4)(C) must be strengthened by requiring businesses to provide contextual information, not just explanations of individual logic. This would empower consumers to recognize if they were treated unfairly and potentially take action. Comment suggests changing the word "may" to "shall," and "or" to "and" in this subsection.	The Agency disagrees with this comment. The access ADMT requirements ensure that consumers have transparency regarding the logic of the ADMT and the outcome of the decisionmaking process for the consumer. The Agency has provided guidance to businesses about how to provide this information, but has not required access to aggregate outputs to simplify implementation for businesses at this time.
Previous 7222(b)(4)(A)–(C)	839	Comment affirms §§ 7222(b)(4)(A)-(C). Comment recommends that the CPPA provide examples in this subsection.	The Agency notes the comment's support. In addition, the Agency has revised the regulations to further simplify implementation for businesses at this time and provide additional guidance on what types of information may be provided regarding the logic of the ADMT and the outcome of the decisionmaking

			process for the consumer. However, the Agency disagrees that additional examples are needed.
Previous 7222(b)(4)(D)	840	Comment suggests that even in the case of security, fraud prevention, or safety purposes, employees, contractors, and gig-workers should be provided with transparency regarding the modality of any surveillance.	The Agency disagrees with this comment, to the extent it argues that workers would not receive sufficient transparency about the use of ADMT to make significant decisions about them. The access ADMT requirements balance providing meaningful information to the consumer in response to an access ADMT request, with ensuring that businesses do not disclose certain security, fraud prevention, and safety information. The Agency does not believe removing or narrowing the exemption regarding security, fraud prevention, and safety is necessary at this time. Additionally, the Agency has removed the other ADMT thresholds regarding extensive profiling and training uses of ADMT to further simplify implementation for businesses at this time.
7222(b)(4)(A) [previously 7222(b)(5)(A)]	1464	Comment recommends deleting the subsection stating that a business can comply by providing a link to the specific section of the business's privacy policy.	The Agency disagrees with this comment. This regulation clarifies how businesses may comply with the instructions requirement and is necessary to ensure that the consumer can clearly distinguish the pertinent information that must be provided to them.
7222(c) [previously 7222(d)]	1465	Comment recommends changing "must not use dark patterns" to say "comply with Section 7004."	The Agency disagrees with this comment. The regulation is clear that a business must not use dark patterns for its submission methods. In addition, the CCPA defines dark patterns, which is further clarified in § 7004. Comment's recommendation is not necessary.
7222(g) [previously 7222(f)]	314	Comment requests clarification on what constitutes "reasonable security measures" for transmitting consumer data, with specific protocols tailored to business size and type. Minimum security standards	The Agency disagrees with this comment. The CCPA requires that businesses implement "reasonable security." (*See* Civ. Code § 1798.100(e).) The regulations are meant to be robust and applicable to

		should be defined to ensure consistency and compliance across industries.	many factual situations and across industries. There is a wide range of factual situations and different industries, and whether a business uses reasonable security measures when transmitting personal information to the consumer is a fact-specific determination. The regulations balance protections for consumers' privacy and flexibility for businesses. This provision is consistent with existing CCPA regulations. (*See, e.g.*, § 7024(f).)
7222(i) [previously 7222(h)]	596, 678	Comment suggests that businesses should not be obligated to require service providers to assist with access requests, as they are already covered by general CCPA obligations. Therefore, § 7222(h) should be deleted. Additionally, forcing service providers to disclose proprietary information is not supported by the CPRA.	The Agency disagrees with this comment. This requirement clarifies the requirements of a service provider or contractor for requests to access ADMT. It also provides service providers and contractors with clear direction of their obligations, while preventing a business from avoiding its obligations for requests to access ADMT by utilizing service providers or contractors. The comment does not explain how the regulation forces service providers to disclose proprietary information in a manner not supported by the CPRA. The Agency does not believe the regulation does so. Rather, the regulation is clear that a service provider or contractor must provide assistance to the business responding to a verifiable request to access ADMT, and provides clarity about what this includes.
7222(j) [previously 7222(i)]	597, 679, 1466	Comment argues that prescriptive requirements when ADMT is used with a consumer more than 4 times in 12 months are unnecessary, too prescriptive, and complex. Therefore, § 7222(j) should be deleted. Alternatively, comment recommends revising subsection to state that an aggregate-level response is allowed for an ADMT that has been used more than two times within a 12-month period.	The Agency disagrees with this comment. § 7222(j), previously § 7222(k), is not a requirement on businesses, but rather provides them with the ability to consolidate responses to requests to access ADMT. A business is not required to consolidate responses by the regulation. Comment's recommendation is not as effective as the regulation at ensuring consumers receive meaningful information about the use of ADMT with respect to them.

7222(k) [previously 7222(j)]	598, 680, 759	Comment states that the CCPA already provides consumers with the general right not to be retaliated against for exercising data subject rights. Therefore, § 7222(j) should be deleted as duplicative and unnecessary.	The Agency disagrees with this comment. § 7222(j) provides clarity because it consolidates the requirements for the right to access ADMT in one place and facilitates compliance with the prohibition against retaliation in the CCPA.
Previous 7222(k)	293, 681, 1570, 1645, 1902	Comment states that § 7222(k) requires businesses to notify consumers of adverse decisions within 15 days and provide detailed explanations within 45 days. This timeline is too short, especially in employment and high-stakes decision-making contexts, where gathering and explaining such information in plain language is resource-intensive. Most of the required information will be of minimal assistance to individuals, and companies will need a "plain language" rendition of the ADMT use in each "adverse significant decision." The Agency should consider revising this section to simplify the process for businesses, or alternatively, to extend the compliance timelines and limit the notice to cases where ADMT played a material role would be more feasible. Comment also argues that this requirement presents several operational challenges in the HR context. The 15-day notice timeline may conflict with existing employment law notice requirements and best practices for handling sensitive employment actions. It may misleadingly suggest that ADMT was the primary driver of the decision, potentially undermining employee trust and complicating workplace relationships. For decisions involving compensation decreases or organizational restructuring, the timing and manner of these notices could create additional workplace tensions.	The Agency disagrees with this comment. The timing and notice requirements balance the burden on businesses with ensuring that consumers receive information about how ADMT was used with respect to them as soon as feasible. Nevertheless, the Agency has removed the notice requirements for "adverse significant decisions" to simplify implementation for businesses at this time.
Previous 7222(k)	599, 760	Comment claims that § 7222(k) establishes an additional notice requirement for certain "adverse	The Agency disagrees with this comment. The notice requirements are flexible and adaptable to a variety of

		significant decisions," which includes "financial or lending" decisions. The additional notice requirements are highly prescriptive and burdensome and should be removed from the final rules.	businesses and situations, and can be incorporated into businesses' existing notice processes. However, the Agency has removed the notice requirements for "adverse significant decisions" to simplify implementation for businesses at this time.
Previous 7222(k)	841	Comment affirms this notice for adverse significant decisions.	The Agency notes the comment's support. However, the Agency has removed the notice requirements for "adverse significant decisions" to simplify implementation for businesses at this time.
Previous 7222(k)	1344, 1942	The requirement to provide an additional adverse significant decision notices, even where a consumer did not request details from the business, exceeds the CPPA's rulemaking authority. Also, the content of the adverse significant decision notices focuses on notifying the consumer that the business reached an adverse significant decision, instead of access to the consumer's personal information. Because the CPPA is constrained to issuing regulations implementing only the specific access right authorized in the statute, the CPPA cannot attempt to create an entirely new CCPA right.	The Agency disagrees with this comment. The Agency has authority to issue rules regarding the right to access ADMT, including ensuring that consumers receive appropriate notices so they can exercise that right. The regulations are consistent with this authority and the intent and purposes of the CCPA. However, the Agency has removed the notice requirements for "adverse significant decisions" to simplify implementation for businesses at this time.
Previous 7222(k)(1)(A)	90, 783, 973, 1685, 1754	Comment recommends expanding the definition of an "adverse significant decision" triggering additional access notice requirements. The current regulations recognize that terminations and pay cuts are significant decisions requiring worker notification. However, other impactful workplace decisions, such as work schedules, pricing, interest rates, disciplinary actions, promotions, shift changes, and involuntary transfers, should also be included in this definition. Comment also argues that businesses should not wait for consumers to request explanations under their right to access in § 7222; instead, these should be provided automatically after an	The Agency disagrees with this comment. The Agency has removed the notice requirements for "adverse significant decisions" to simplify implementation for businesses at this time. However, the regulations continue to require a Pre-use Notice, so that consumers are notified of their access and opt-out rights and provided with necessary information to meaningfully exercise those rights. Businesses also may provide additional contextual information beyond what is required in § 7222(b) in response to an access ADMT request.

		adverse significant decision was made about them. In addition, comment states that the post-use notice is only valuable to consumers if it is actionable. Without understanding how they compare to other consumers, consumers faced with adverse ADMT decisions will not know whether they should pursue additional action. The regulations should be changed to require businesses to provide contextual information.	
ADMT	1, 3	Comment states the proposed regulations undermine consumer privacy expectations by imposing unnecessary disclosures about ADMTs, creating additional barriers between customers and the services they have agreed to receive. Comment also states the proposed regulations undermine privacy by causing notice fatigue through excessive interruptions, eroding trust in privacy notices and hindering meaningful privacy dialogue.	The Agency disagrees with this comment. The regulations do not impose unnecessary disclosures about ADMTs or create additional barriers between customers and services. The regulations ensure that consumers receive disclosures when necessary to exercise their CCPA rights with respect to ADMT and can meaningfully exercise these rights. They also provide flexibility to businesses with respect to how to provide these disclosures and access/opt-out mechanisms to consumers.
ADMT	8, 219	Comment suggests the Agency withdraw all ADMT regulations and instead address the ADMT requirements as part of broader requirements that relate to privacy.	The Agency disagrees with the recommendation to withdraw the ADMT regulations. Comment's suggestion that the ADMT regulations are not related to privacy is inconsistent with the CCPA, which includes opt-out and access rights with respect to the use of ADMT as part of the CCPA's privacy protections for consumers.
ADMT	85	Comment supports key definitions and coverage concepts in the regulations regarding ADMTs. This includes the explication of "significant decisions" and "extensive profiling" in the employment context. Comment recommends not narrowing these terms in future revisions.	The Agency notes the comment's support for the regulations. The Agency has revised the definition of significant decision to provide additional clarity and to simplify implementation for businesses at this time. Similarly, the Agency has removed the term "extensive profiling" in Article 11 to simplify implementation at this time. However, the Agency has retained the requirement to conduct a risk assessment for certain

			uses of automated processing in the workplace and in sensitive locations. These uses of automated processing pose significant risk to consumers' privacy and require a risk assessment.
ADMT	86, 87	Comment suggests that the widespread use of algorithmic decision-making in workplaces is often hidden from both policymakers and workers, making it difficult for employees to understand how decisions are made. Workers should be informed about the ADMTs used in their workplace, including the types of ADMTs used to make critical decisions, which traits or attributes the ADMTs analyzed, and the methods by which they measure those traits or attributes. This transparency is important for ADMTs that require the worker to input information or otherwise interact with the ADMT, citing an example of workers with disabilities requesting accommodation. Comment argues that once ADMTs have been used to make an employment-related decision, workers should have the right to know what model was used, what the inputs were, and crucially, what the outputs were and how the employer used them. Some ADMTs rely on unreliable data, such as customer ratings, which are prone to racial, gender, and linguistic biases. Without transparency, workers remain unaware of how their performance evaluations are influenced by biased systems, making it difficult to challenge unfair treatment.	The Agency agrees with this comment in part. Transparency and protection against discrimination are necessary to protect consumer privacy. The Pre-use Notice requirements ensure that consumers have necessary information before they exercise their ADMT rights. The ADMT access requirements ensure that consumers have information about how the ADMT was used to make a decision concerning them. With respect to discrimination, businesses must identify risks to consumers' privacy, which may include unlawful discrimination, prior to using the ADMT. The Agency disagrees with this comment in part. To the extent the comment is recommending more information be included in the Pre-use Notice and access ADMT requirements or risk assessment requirements, the Agency disagrees that this is necessary at this time. The Agency believes that these requirements, as revised, are sufficient and appropriate to simplify implementation for businesses at this time while providing additional transparency and protection against discrimination for consumers.
ADMT	88	Comment believes that providing workers with notice of ADMT use can be streamlined into existing processes, such as during hiring or onboarding, and through automated updates. These measures align with established notice requirements under the CCPA and	The Agency agrees with this comment. The Pre-use Notice requirements can be streamlined into existing processes, such as through the Notice at Collection or through consolidated notices. These ensure meaningful transparency to consumers while

		should not be considered overly burdensome for employers.	providing flexibility to businesses in meeting their compliance obligations.
ADMT	118, 1063, 1242, 1943, 1946, 1961	Comment argues that the regulations could harm their business, which relies on data-powered and automated decision-making tools to connect with customers. For example, if customers face multiple pop-ups or opt-out mechanisms on the way to a site, many will likely leave before even engaging with the content, reducing website visitors, store visits, sales, and access to essential products. Consumers will be driven to out-of-state business not covered by these regulations. Comment also believes that the regulations fail to recognize the benefits of ADMT tools for small businesses and could stifle growth. Small businesses rely heavily on data-powered and automated decision-making tools to level the playing field against larger competitors. The new rules make it harder and more expensive for CA small businesses to advertise to interested customers. They place first party advertising into the same category as high-impact ADMT.	The Agency disagrees with this comment. With respect to pop-ups and opt-out mechanisms, the regulations provide flexibility for businesses on consolidating notices, as indicated in §§ 7220(a) and (e), and in providing opt-outs to consumers, as indicated in 7221. In addition, to the extent this comment is related to the opt-out of profiling for behavioral advertising, that requirement has been removed. With respect to the impact on small businesses, the regulations balance providing protections for consumers' privacy while providing flexibility businesses. The regulations have also been revised to further simplify implementation for businesses, including small businesses, at this time.
ADMT	123	Comment argues that the regulations, while targeting automated decision-making, would apply to mainstream technologies that aid human decision-making rather than fully automating it. This includes technologies that involve significant human oversight. These rules should be focused on truly automated systems that operate without human control, as otherwise it is out of step with other frameworks and would impose new burdens.	The Agency agrees with this comment in part, to the extent it requests narrowing the definition of ADMT to exclude uses with human involvement. The Agency otherwise disagrees with the comment. The regulations are consistent with approaches taken in other jurisdictions and are not unduly burdensome. They balance providing privacy protections for consumers with flexibility for businesses to come into compliance.
ADMT	131, 294, 550	Comment argues that the regulations will create unnecessary disclosures. The regulations could unduly interfere with consumer use of the internet and result in frustrated consumers leaving a site before completing a	The Agency disagrees with this comment. The regulations ensure that consumers have meaningful information when necessary to exercise their CCPA rights and provide flexibility to businesses with

		transaction, or leaving before the business could share important information with users. Potential customers opting out of data collection or encountering confusing pop-ups may prevent businesses from reaching and informing them about their services. The regulations will also hinder the ability of startups to use data- and ADMT-powered tools to connect with target customers, particularly decision-makers in large enterprises. Comment also recommends focusing on uses of ADMT with consequential decisions to avoid discouraging businesses from using AI.	respect to providing relevant notices and opt-out or similar mechanisms to consumers. With respect to pop-ups and opt-out mechanisms, the regulations provide flexibility for businesses on consolidating notices, as indicated in §§ 7220(a) and (e), and in providing opt-outs to consumers, as indicated in 7221. However, exercising its discretion, the Agency has revised the ADMT regulations to focus on significant decisions, which further simplifies implementation for businesses at this time.
ADMT	146, 1320, 1467, 1538, 2040	Comment asserts that the Agency is exceeding its statutory mandate under the CCPA by attempting to regulate AI and automated decision-making broadly. Comment argues that the inclusion of AI and ADMT in the regulations fail to satisfy the authority standard under Government Code § 11349(b). Comment argues that AI governance should be determined by the legislature, not the Agency, as evidenced by Governor Newsom's veto of an AI-related bill. Additionally, comment claims that employment-related automation decisions should be regulated by specialized labor agencies rather than through privacy rules.	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, it is required to issue regulations and impose certain requirements. Moreover, the Agency engaged in robust preliminary rulemaking activities with a variety of stakeholders and has collaborated with state law makers and will continue to do so, consistent with the CCPA's direction to the Agency. (*See* Civ. Code § 1798.199.40(g).) Nevertheless, exercising its discretion, the Agency has deleted the definition of artificial intelligence and removed corresponding references throughout the regulations to further simplify implementation for businesses at this time. With respect to employment decisions, the CCPA explicitly provides privacy protections to employees. Comment's suggestion to

			remove employment decisions from the regulations is inconsistent with the CCPA.
ADMT	147	Comment claims that the Agency's proposed rules improperly regulate the underlying technology of automated decision-making rather than focusing solely on the processing of personal information, which is the Agency's actual mandate. It argues that such overreach extends beyond the scope of the CCPA. Additionally, comment claims that employment-related automation decisions should be regulated by specialized labor agencies rather than through privacy rules.	The Agency disagrees with this comment. The regulations must define the term "automated decisionmaking technology" to provide clarity for businesses. This term also explicitly applies to the processing of personal information. (*See* Civ. Code § 1798.185(a)(15); § 7001(e).) In addition, issuing these rules is within the Agency's delegated authority under the CCPA, and furthers the intent and purpose of the law. With respect to employment decisions, the CCPA explicitly provides privacy protections to employees. Comment's suggestion to remove employment decisions from the regulations is inconsistent with the CCPA.
ADMT	160	Comment asserts that even if the proposed regulations are improved, banks will need at least 24 months to assess their ADMT systems, implement compliance mechanisms, and align their processes with federal regulations. A rushed implementation could lead to confusion and unintended consequences.	The Agency disagrees with this comment, to the extent the comment argues that the regulations would lead to a rushed implementation. However, exercising its discretion, the Agency has added § 7200(b) to provide businesses until January 1, 2027 to come into compliance with the ADMT requirements in Article 11.
ADMT	222	Comment acknowledges the CPPA's effort to enhance consumer privacy but highlights concerns with the practical aspects of the regulations, suggesting that the Agency should clarify the scope of the regulations on automated decisionmaking technology and revise how they work in practice.	The Agency disagrees with this comment, to the extent it suggests that the regulations are not clear. The regulations are clear about their scope and requirements. In addition, the Agency has revised the regulations to further simplify implementation for businesses at this time.
ADMT	301	Comment argues that the regulations, specifically opt-out provisions for training, risk diminishing the quality and accuracy of ADMTs by reducing the size and diversity of training data. As a result, opt-outs could	The Agency disagrees with this comment. The regulations would not reduce the quality or accuracy of ADMTs. They also balance providing consumers with privacy protections with flexibility for businesses to come into compliance. In addition, the regulations

		lead to less effective AI products, negatively impacting outcomes like health and safety.	have been revised, including removing the opt-out of training uses of ADMT, to further simplify implementation for businesses at this time.
ADMT	303, 1256	Comment states that the ADMT regulations are overly broad and exceed the Agency's authority. Comment argues that the Agency's regulations create a fragmented regulatory landscape that conflicts with emerging national AI governance efforts. Instead of coordinating with federal initiatives, these rules impose additional compliance costs and uncertainty on businesses. Specifically, the proposed regulations contradict the House AI Task Force's bipartisan framework, which supports domain-specific AI regulation and federal preemption to avoid state-by-state fragmentation. Businesses operating in multiple states will face overlapping and contradictory regulations, making compliance more complex and expensive. Comment advocates for a preemptive federal privacy law to avoid a patchwork of regulations.	The Agency disagrees with this comment. The ADMT regulations are within the Agency's authority and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a).) The regulations harmonize with other frameworks while furthering the intent and purposes of the CCPA and providing clarity for businesses regarding their obligations. The regulations also enable businesses to leverage existing compliance processes to comply with the requirements. Nevertheless, the definition of significant decision and § 7200 have been revised to focus on the use of ADMT for significant decisions and references to AI have been removed to further simplify implementation at this time. The Agency does not have authority over federal law and is required to implement California's privacy law, the CCPA.
ADMT	361, 458, 785	Comment argues that the proposed ADMT regulations exceed the Agency's statutory authority and duplicate existing efforts in California, particularly by the California Civil Rights Department ("CRD"), who is finalizing employment-related AI regulations. The overlapping regulations create compliance difficulties and potential conflicts. Additionally, AB 2930, which previously sought to regulate AI and ADMT, may be reintroduced in 2025, further complicating compliance. The inclusion of employees and job applicants under consumer privacy laws like the CPPA adds confusion and increases compliance costs for businesses. Comment argues that AI and ADMT regulation in	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) Also, the CCPA includes workers within its scope. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, it is required to issue regulations and impose certain requirements. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. Nevertheless, exercising its discretion, the Agency has

		employment should be handled by the legislature or the CRD, rather than the CPPA. The CPPA should cease rulemaking on ADMT until granted explicit statutory authority.	removed references to artificial intelligence to further simplify implementation for businesses at this time. The regulations are also consistent with the approach taken by the CRD. The Agency looks forward to working with stakeholders, including the Legislature and Governor Newsom, on future policy development.
ADMT	443	Comment advocates for clear guidance on how consumers can access the complaint system through the CPPA's website, ensuring transparency in enforcement procedures. This would provide consumers with a straightforward mechanism for addressing concerns related to ADMT.	While not on the proposed action, the Agency notes commenter's suggestion and looks forward to working with stakeholders on future policy development.
ADMT	441	Ensure the plain language explanations include: "§ 7003. Requirements for Disclosures and Communications to Consumers. (a) Disclosures and communications to consumers shall be easy to read and understandable to consumers. For example, they shall use plain, straightforward language and avoid technical or legal jargon. The logic and purpose of the AI system. The potential impacts, risks, and ethical considerations associated with its use. Examples of permitted and prohibited uses."	The Agency agrees in part with this comment, to the extent it supports compliance with § 7003 when providing disclosures to consumers and providing information to consumers regarding the purposes, logic, and outcome of decisionmaking processes. The Agency disagrees in part with this comment, to the extent that it recommends additional requirements beyond what it is in the regulations. Disclosures and communications to consumers must already comply with § 7003. The regulations balance providing transparency to consumers to ensure they can exercise their CCPA rights with the burden on businesses.
ADMT	444, 445, 555	Comment recommends that the Agency mandate data minimization and purpose limitation for the use of ADMT. This would ensure that businesses only collect data that is necessary for a specific, legitimate purpose, and restricts the repurposing of data for unrelated uses without explicit consumer consent. Comment also suggests that the CCPA should align with the European Data Protection Board's (EDPB) December 2024	The Agency disagrees with this comment, to the extent it argues that businesses do not already need to comply with § 7002. § 7002 already requires businesses' use of consumers' personal information to be necessary and proportionate, and provides clear rules regarding how they can do so, including requirements regarding the minimum personal information to achieve the purpose of the processing

		guidance on processing personal data in AI models, emphasizing the use of Legitimate Interest, Necessity Tests, and Balancing Tests. These guidelines align with § 7154.	and when consent must be obtained. This applies to business's use of ADMT. § 7154 has also been revised to clarify the goal of the risk assessment, which provides clear guidance to businesses and is consistent with the CCPA's plain language.
ADMT	446	Comment recommends incorporating Privacy-Enhancing Techniques (PETs) to minimize data collection, anonymize consumer data, and ensure that data is not transferred without authorization. PETs should be implemented not only by the AI deployers but also by third-party entities involved in the ADMT ecosystem. These safeguards are intended to ensure the privacy and security of personal data and build public trust in AI technologies.	The Agency disagrees with this comment, to the extent it argues that businesses do not already need to comply with § 7002. § 7002 already requires businesses' use of consumers' personal information to be necessary and proportionate, and provides clear rules regarding how they can do so, including requirements regarding the minimum personal information to achieve the purpose of the processing and when consent must be obtained. This applies to a business's use of ADMT. Mandatory incorporation of PETs is not necessary at this time. Businesses may consider a variety of safeguards in their processing, including the use of PETs, as outlined in § 7152(a)(6).
ADMT	447	Comment calls for businesses to assess whether AI models trained on personal data can be classified as anonymous. They stress that for an AI model to be considered anonymous, the risk of extracting personal data should be extremely low, and the model must be resistant to data extraction attacks. Furthermore, businesses should document measures to prevent or limit personal data collection during AI training. Additionally, comment advocates for algorithmic risk assessments to ensure compliance with data minimization and proportionality standards.	The Agency disagrees with this comment, to the extent that it argues that the CCPA or the regulations do not address its recommendations. The CCPA provides clear definitions of "deidentified" and "aggregate consumer information" that businesses must meet if they seek to deidentify or aggregate consumers' information under the CCPA. Additionally, § 7002 already requires businesses' use of consumers' personal information to be necessary and proportionate, and provides clear rules regarding how they can do so, including requirements regarding the minimum personal information to achieve the purpose of the processing. Businesses must also document relevant safeguards when conducting risk assessments. Further, businesses must conduct risk

			assessments for certain uses of ADMT, training uses of personal information, or automated processing. These risk assessment requirements ensure that businesses identify relevant risks to consumers' privacy. The Agency does not believe that additional requirements are necessary at this time.
ADMT	448, 556	Comment recommends the Agency establish standardized incident reporting mechanisms to ensure consistent, transparent, and actionable documentation of ADMT system failures and problems. These incident reports should be compiled in a publicly accessible database with clear categories for analysis. The recommendation aligns with global best practices, specifically the OECD's comprehensive frameworks for AI incidents. This would enable the Agency to collect consistent data on failures, biases and harms across businesses using ADMT, and identify recurring issues, systemic risks, or predatory privacy practices.	The Agency disagrees with this comment. Businesses must conduct risk assessments and submit relevant risk assessment information and reports to the Agency. These requirements comply with the directive to the Agency in the CCPA. The Agency does not believe an incident reporting mechanism is necessary at this time.
ADMT	451, 557	Comment urges the Agency to prohibit the use of children's data for ADMT training due to risks of exploitation and harm, emphasizing that children's data is vulnerable to being misused for profiling and AI training without parental consent. Comment references the FTC's actions to prevent monetization of children's data and a case where children's photos were used in AI training without consent, reinforcing the necessity of stronger privacy measures. The recommendation includes limiting the collection and use of children's data to necessary purposes only and ensuring that such data is not repurposed for ADMT training without explicit consent. Comment also suggests regular impact assessments for such systems.	The Agency disagrees with this comment. § 7002 already requires businesses' use of consumers' personal information to be necessary and proportionate, and provides clear rules regarding how they can do so, including requirements regarding the minimum personal information to achieve the purpose of the processing and when consent must be obtained. In addition, the regulations now define sensitive personal information to include personal information of consumers that the business has actual knowledge are less than 16 years of age. Further, businesses must conduct risk assessments when processing sensitive personal information, and uses of sensitive personal information are subject to the CCPA's requirements for the right to limit.

ADMT	157, 228	Comment emphasizes that financial institutions have relied on ADMT for years under strict federal regulations. Automated tools improve efficiency, accuracy, and security in lending, fraud detection, and compliance without the need for additional state-level oversight. The breadth of the ADMT regulations and the lack of appropriate limitations on the requirements and rights created by the rules would impede these long-standing and common practices. Comment states that the regulations require businesses to comply with sweeping obligations before using ADMT for significant decisions, extensive profiling of a consumer, or training certain uses of ADMT. These requirements present several concerns. The Agency should address practical concerns with requirements for Pre-use Notices, opt-outs of ADMT, and requests to access ADMT.	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The regulations balance providing privacy protections for consumers with flexibility for businesses to come into compliance. The regulations have also been revised to further simplify implementation for businesses at this time.
ADMT	159, 186, 1028	Comment asserts that while the rules recognize the need for fraud prevention exemptions, they do not go far enough. The regulations should be amended to more clearly exempt fraud detection practices and remove any requirements which may impede fraud detection by financial institutions. Banks must be allowed to use fraudsters' data to train security models, or these models will become ineffective over time. Additionally, requiring detailed notices for fraud-related ADMT decisions could help fraudsters refine their evasion tactics. Comment recommends adding an exception for businesses having to comply with Article 11 where such compliance would compromise its use of ADMT for security, fraud prevention, or safety purposes; or would compromise processes to comply with laws to which the business is subject.	The Agency disagrees with this comment. The Agency modified the definition of ADMT to focus on a higher-risk use of ADMT at this time, which is a use without any human involvement. Separately, the Agency revised the definition of significant decision and revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. The Agency has accordingly removed the security/fraud-prevention/safety exception from the ADMT opt-out exceptions as unnecessary. The regulations also clarify that a business is not required to include certain information related to security, fraud prevention, or safety in the information required in the Pre-use Notice, nor in the information required in response to a consumer's request to access ADMT. With respect to training ADMT, this threshold has

			been removed from Article 11. The fraud prevention provision in §§ 7220 and 7222 has been revised to address malicious, deceptive, fraudulent, or illegal actions directed at consumers as well as the business. These regulations address comment's concern about providing detailed notices that could help fraudsters. The regulations balance providing protections for consumers to meaningfully exercise their ADMT rights while making clear that businesses do not need to provide detailed information about fraud prevention. These modifications also balance protections for consumer privacy and simplifies implementation for businesses at this time. Businesses may still deny fraudulent requests to opt out of ADMT as set forth in § 7221(g).
ADMT	438	Comment applauds California's proactive leadership in ensuring the responsible development and deployment of AI technologies, particularly in addressing high-risk applications of ADMT that may adversely impact individuals' lives and fundamental rights with profound ethical consequences. The CPPA has developed a comprehensive framework to regulate the risks of ADMT. Commenter's recommendations aim to further strengthen CCPA's impact on public safety.	The Agency agrees with this comment, to the extent it supports the regulations. Additional modifications are not necessary at this time.
ADMT	500, 1870	Comment argues that the definition of ADMT is overly broad. The definition fails to account for the heterogeneity of AI systems and the nuanced ways they may function across industries. Comment warns that treating all computational technologies as "high risk" could harm AI development. Comment also warns that this overreach creates significant uncertainty for businesses, particularly small and mid-sized firms. Comment suggests the Agency to adopt a narrower,	The Agency disagrees with this comment. The ADMT regulations are within the Agency's authority and further the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT but does not define ADMT. (*See* Civ. Code § 1798.185(a).) The regulations also do not treat all computational technologies as high risk. However, exercising its discretion, the Agency has revised the

		risk-based framework focusing on truly consequential uses of ADMT (which may or may not involve AI), while allowing routine and low-risk applications to continue delivering economic and societal benefits. A more targeted approach would align California's efforts with evolving federal and global frameworks, while preserving the state's position as a leader in AI development and innovation.	definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and § 7200, to focus on the use of ADMT for significant decisions to simplify implementation at this time. As revised, the regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. With respect to artificial intelligence, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time.
ADMT	545	Comment supports the Agency's proposed regulations, emphasizing the need for strong protections for workers and renters. Comment argues that ADMT can impact wages, job security, and housing access, particularly for vulnerable communities. Comment backs consumer opt-out rights and sees the regulations as an opportunity for California to lead in AI governance.	The Agency agrees with this comment and notes commenter's support.
ADMT	546	Comment expresses strong support for the Agency's efforts to regulate ADMT. Comment highlights concerns over Californians' personal data being repurposed for AI training without adequate transparency or recourse.	The Agency agrees with this comment and notes commenter's support. However, the Agency has removed the training threshold from Article 11, to simplify implementation for businesses at this time.
ADMT	554	Comment urges the Agency to enforce the purpose limitation principle, specifically for the use of ADMT in significant decisions.	The Agency disagrees with this comment, to the extent it argues that the Agency does not enforce the requirements of § 7002, which addresses requirements for businesses' use of personal

			information. This would apply to using ADMT to make a significant decision concerning a consumer. As with other violations of the CCPA, the Agency has enforcement authority if a business is not complying with the law.
ADMT	558	Comment opposes the proposed ADMT regulations, arguing they will negatively impact California businesses.	The Agency disagrees with this comment. The regulations are issued pursuant to the CCPA's delegation of authority to the Agency. In addition, the Agency has made efforts to limit the burden of the regulations while implementing the CCPA.
ADMT	666	Comment argues that requiring disclosure, opt-out rights, and logic explanations for ADMT training uses imposes unnecessary burdens. Since training does not involve actual decision-making about consumers, these requirements would result in "notice fatigue" and slow down essential service delivery. Comment recommends removing training-related ADMT uses from the regulation.	The Agency disagrees that the requirements for training uses of ADMT would impose unnecessary burdens on businesses. However, the Agency has removed this threshold from Article 11 to simplify implementation for businesses at this time.
ADMT	712	The Agency should make clarifications because the proposed regulations are difficult in practice. For example, an opt-out for underwriting and rating decisions would be impractical. The Agency should modify the definition of "significant decision," and remove from the definition of ADMT the following language: "or substantially facilitate human decision-making." Comment argues that ADMT should be limited to those technologies (such as machine learning models, natural language processing, robotics, and computer vision technologies) where there is no human involvement in the ultimate, significant decision. The regulations should also not apply to behavioral	The Agency disagrees with the comment. The Agency modified the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time.

		advertising and marketing activities because these are not "significant decisions" impacting consumers.	
ADMT	780	Comment agrees that the proposed regulations appropriately extend existing consumer rights (deletion, correction, knowledge, and limitation) to ADMT access and appeals, improving transparency through mandatory reporting on opt-out and access requests. The opt-out right exclusions also correctly do not apply to behavioral advertising and training ADMT uses.	The Agency notes this comment of support. However, the Agency revised the regulations to simplify implementation for businesses at this time, including removing the threshold for behavioral advertising and training ADMT and corresponding opt-out provisions in Article 11.
ADMT	817	Comment suggests that when the output from the ADMT is or involves personal information then the rights of consumers must be upheld. However, if personal information is involved in the training, testing and validation dataset but cannot be replicated or reproduced in the outputs of the ADMT, then the rights of consumers need not be applied to those datasets.	The Agency agrees with this comment, to the extent it supports the CCPA rights that consumers have with respect to their personal information. With respect to training uses of ADMT, the Agency has revised the regulations to remove this threshold from Article 11.
ADMT	832	Comment believes that the human appeal process is only useful in the circumstance where time is not of the essence. In certain circumstances, the human appeals process may result in thousands of appeals, for example ADMT for resume screening. Comment suggests if all applicants seek human review/appeal for every resume they submit, the system will collapse. Comment suggests human oversight requirements, and provision of transparency and explainability prior to the consumer interacting with the ADMT.	The Agency disagrees with this comment. The revised proposed regulations balance privacy protections for consumers, including protecting them against excessive wait times, and flexibility for businesses regarding how to address consumers' concerns about the use of ADMT to make significant decisions about them. The timeline for requests to appeal is consistent with existing timelines to respond to other CCPA requests. (*See* § 7021.) The regulations ensure that consumers have meaningful information about use the of ADMT with respect to them when they are exercising their CCPA rights. (*See* § 7220.) In addition, hiring decisions are subject to a separate opt-out exception in § 7221(b)(2), which also addresses comment's concerns about feasibility. Human oversight, transparency, and explainability help more effectively ensure consumer control over their

			personal information when they supplement, rather than replace, the opt-out requirements in § 7221.
ADMT	833, 834, 1615, 1640	Comment states that most organizations are not equipped to assess bias mitigation in training, testing, and validation datasets, partly because ADMT providers themselves fail to address bias adequately. These tools often exclude qualified candidates due to semantic errors rather than actual qualifications, leading to widespread distrust among job seekers. Furthermore, ADMT systems claim to assess emotional and psychological traits for hiring decisions, despite lacking sufficient scientific validity. Increasing transparency and explainability in these tools could help mitigate their exclusionary impact and refocus hiring decisions on genuine qualifications. Comment argues that § 7221(b)(4) does not contain the requirement of a bias assessment mentioned in the previous subsections. Comment criticizes the exemption from direct evaluation using third-party ADMT under §§ 7201(a)(1)(A), 7221(b)(3)(B)(i), (b)(4)(B)(i), (b)(5)(B)(i). Comment argues that while a developer's evaluation can inform deployment, the responsibility for evaluating fairness, accuracy, and discrimination must ultimately lie with the deploying business, as these risks are highly context-specific. Both ADMT developers and deployers share responsibility for ensuring fairness and accuracy. The proposed regulations should acknowledge that businesses will at times need to test ADMT systems using representative samples to ensure their use of ADMT does not discriminate. Comment argues that requiring evaluations and safeguards for work/educational profiling is too costly and impractical,	The Agency disagrees with this comment. The Agency revised the definition of significant decision and revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. These revisions include removing references to "work or educational profiling" from § 7221, and the corresponding opt-out exception. With respect to the exception for admissions, acceptance and hiring decisions in § 7221(b)(2)(B), previously § 7221(b)(3)(B), the Agency has removed the requirement that the ADMT be "necessary to achieve" the purposes set forth in those subsections, to simplify implementation for businesses at this time. However, the Agency has retained the requirement that the ADMT be used "solely for" the purpose. The Agency also removed the evaluation and safeguard-implementation requirements to ensure the ADMT works as intended for the business's proposed use and does not discriminate based upon protected classes, to simplify implementation for businesses at this time. The Agency retained the requirements that the ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics. These revisions balance protections for consumer privacy and simplifying implementation for businesses at this time. Regarding the comment's suggestion that there was a difference in bias-assessment between §§ 7221(b)(2)(B) and (3)(B), previously § 7221(b)(3)(B) and (4)(B), the comment's interpretation of the regulation is inconsistent with the proposed regulations' language. The subsections require businesses to provide the same protections;

		especially since the term "work profiling" is not clearly defined.	the difference had been that § 7221(b)(4)(B) had used the abbreviation created in § 7221(b)(3)(B). Further, the Agency has deleted § 7201, which imposed requirements for physical or biological identification or profiling, to simplify implementation at this time.
ADMT	763, 873, 874, 1210, 1327	Comment asserts that the regulations exceed the Agency's authority to issue privacy rules, which only contemplates rulemaking related to existing access and opt-out rights. The regulations improperly enlarge the statutory scope to cover bias, explainability, model training, and other risks addressed in broader AI frameworks. They fail to distinguish between significant and non-significant decisions. They also set forth rules where other CA agencies have authority and have issued requirements (e.g., CA Civil Rights Department issued regulations to protect against employment discrimination with ADMT). If the Agency pursues extra-statutory ADMT and AI regulation, it should at least align with the underlying scope of the statute and/or align with other state privacy frameworks for purposes of interoperability. Comment claims that the proposed regulations diverge from regulatory approaches in the EU AI Act and the Colorado AI Act, both of which recognize the unique role of general-purpose AI models. Those laws impose transparency requirements rather than subjecting developers to compliance obligations meant for deployers. Comment calls for a risk-based framework similar to the Colorado AI law and EU AI Act, which tailor obligations based on the potential for consumer harm.	The Agency disagrees with this comment. The regulations are within the Agency's authority under the CCPA. (*See* Civ. Code §§ 1798.185(a)(14)-(15).) In addition, the commenter's interpretation of the access and opt-out rights for ADMT and arguments that regulating AI is beyond the Agency's authority are inconsistent with the text of the CCPA, which the legislature explicitly amended to state that personal information can exist in artificial intelligence systems. Nevertheless, exercising its discretion, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time. Additionally, both the text and purpose of the CCPA support preventing discrimination against consumers and address processing that present significant risk to consumers' privacy, which includes training uses. Contrary to commenters assertion, the regulations do not require explainability, but rather compliance with the access ADMT requirements, which is explicitly required by the CCPA. The regulations are consistent with the requirements of the California Civil Rights Department and other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity and guidance to businesses regarding their obligations.

ADMT	929	Comment argues that the Agency's proposal to create ADMT-specific access and opt-out rights exceeds its statutory authority under Civil Code § 1798.185(a)(15), which only allows clarification of existing statutory rights rather than creating new ones. Additionally, relying on a single statutory sentence to establish these rights constitutes an unconstitutional delegation of legislative authority. The legislature and voters must first define these rights before the Agency implements regulations.	The Agency disagrees with this comment. Proposition 24, which was approved by voters in 2020, provided authority to the Agency to issue regulations regarding access and opt-out rights with respect to ADMT. Proposition 24 also provides clear guidance to the Agency regarding the implementation of the CCPA. The CCPA directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code §§ 1798.185(a)(15).) The regulations are within the Agency's authority and further the intent and purpose of the CCPA.
ADMT	976	Comment supports that the regulations on ADMT are necessary and are not overly burdensome. Businesses choose to use ADMT for cost-saving purposes, and those benefits should be balanced by protections for consumers. Increases in productivity require additional measures to ensure there are not harms and are fungible benefits for all. These regulations are a step in that direction and should be seen as such.	The Agency agrees with this comment, to the extent it supports the regulations.
ADMT	1001, 1003, 1004, 1005	Comment acknowledges the Agency's efforts but expresses concern that the proposed rule may negatively impact patient care due to existing FDA regulations on AI/ML in medical devices. AI in medical technology is already regulated under FDA's rigorous standards, which include reviewing bias mitigation. Adding state regulations could create conflicting requirements and uncertainty, potentially delaying market access for beneficial AI-driven medical advancements. Medical AI is often designed to assist in high-frequency diagnostic tasks (like imaging). The draft rules oversight requirements would make real-time decision-making harder, add delays in care, and	The Agency disagrees with this comment. The CCPA includes certain data-level exemptions. However, it applies to "businesses" and directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The CCPA makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196.) The Agency has made efforts to limit the

		undermine provider ability to respond to new clinical problems. The opt-out requirement for ADMT could interfere with medical device servicing and clinical workflows, particularly for devices requiring continuous data collection (e.g., implants, ER equipment). Comment proposes that the regulations explicitly exempt AI systems already regulated under the Federal Food, Drug, and Cosmetic Act to avoid unnecessary regulatory overlap. Comment proposes language: "The requirements in this chapter shall not apply to artificial intelligence systems that are subject to applicable requirements pursuant to the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321 et seq.)."	burden of the regulations while implementing the CCPA. In addition, exercising its discretion, the Agency also deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time. Finally, the Agency has revised the ADMT regulations to focus on the use of ADMT for significant decisions to simplify implementation at this time.
ADMT	1008	Comment opposes the inclusion of AI in the ADMT regulations, arguing that it assumes AI is inherently harmful and could stifle technological advancements and economic growth.	The Agency disagrees with this comment. Nevertheless, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time.
ADMT	1013, 1126, 1220, 1222, 1230, 1234, 1477, 1481, 1581, 1762, 1872, 1893	Comment questions whether the proposed regulations will meaningfully enhance consumer privacy and argues that the compliance burden may outweigh any potential benefits. Comment commends the Agency's efforts to enhance consumer privacy and data protection, but urges the Agency to pursue a balanced approach that promotes the responsible use of AI, while preventing potential algorithmic discrimination. Comment argues that the proposed rule's level of detail and "one-size-fits-all" approach would impose unnecessary regulatory burdens on credit unions without improving consumer privacy or security. Comment warns that the Agency should ensure that its proposed regulations do not overburden businesses that develop or deploy ADMTs,	The Agency disagrees with this comment. The regulations balance providing privacy protections to consumers with flexibility for businesses to come into compliance. The regulations also harmonize with other jurisdictions, such as Colorado, while furthering the intent and purpose of the CCPA. In addition, the regulations provided clarity and guidance to businesses regarding the scope of their obligations. The regulations have also been revised to further simplify implementation for businesses at this time. Also, the Agency has appropriately considered the impact on businesses and innovation and has made efforts to limit the burden of the regulations while implementing the CCPA. The Agency engaged in

		as businesses must already contend with a growing patchwork of statutes, regulations, and commitments, such as AB 2013 and state laws from Colorado and Utah. Comment emphasizes that while consumer privacy protections are important, they must be carefully designed and narrowly tailored. Overly broad rules could unintentionally harm the very consumers they aim to protect by restricting beneficial uses of AI. Comment urges the Agency to narrow the proposed rules to address real privacy risks without imposing broad burdens that harm consumers through higher prices and reduced choice. Comment also recommends creating regulatory obligations that businesses can meaningfully operationalize. Given that the use of AI can reduce biased outcomes by applying objective criteria, particularly when a human oversees the decision process, comment warns that restricting AI could undermine fairer decisionmaking processes. Comment claims that the proposed regulations fail to account for the different roles in AI development and deployment. Developers, integrators, and deployers leverage AI models and tools for their own innovative purposes, and each have different capabilities to mitigate risks. They should not be regulated identically. Regulatory standards should identify relevant participants in the ecosystem and allocate appropriate responsibilities and obligations to each of them. Comment also states that small businesses heavily rely on AI tools to compete, grow, and survive. The broad regulations risk subjecting routine AI tools to onerous compliance requirements. The cost of compliance could become a barrier for small businesses to adopt AI technologies, particularly given that AI tools provide the greatest productivity benefits to more modestly	robust preliminary and formal rulemaking activities with a wide variety of stakeholders and has collaborated with state lawmakers and will continue to do so, consistent with the CCPA's direction to the Agency. (*See* Civ. Code § 1798.199.40(g).) The resulting regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Nevertheless, the Agency has modified the regulations to significantly reduce their costs. Lastly, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time.

		resourced workers and businesses. This regulatory burden would not only stifle innovation but could also exacerbate existing challenges that small businesses already face.	
ADMT	1056	Comment encourages more detailed guidance on the application of ADMT rules to deepfake technologies to ensure they target malicious uses without hindering legitimate AI innovation.	The Agency disagrees with this comment. The regulations regarding deepfakes are reasonably clear. However, the Agency has removed the term "deepfake" and corresponding requirements from the regulations to further simplify implementation for businesses at this time.
ADMT	1057	Comment argues that the expanded definitions of "agent" and "employment agency" could unfairly hold third-party vendors and platforms responsible for discrimination risks beyond their control. Service providers might be forced to halt business operations to avoid potential legal liability.	The Agency disagrees with this comment. The regulations do not define the terms "agent" or "employment agency." To the extent that the commenter raises concerns about the requirements for service providers and third parties, the CCPA and regulations are clear about the scope of their obligations to protect consumer privacy. The Agency disagrees that these obligations could unfairly hold vendors responsible for discrimination risks beyond their control.
ADMT	1070, 1071, 1079, 1080	Comment proposes strengthening notice and access rights to ensure individuals, including workers, have transparency when an ADMT has been used to make a decision affecting them. This promotes transparency and fairness. Comment supports restoring a meaningful right for workers and consumers to opt out of consequential ADMT systems, ensuring individuals have control over decisions that impact their livelihoods.	The Agency agrees in part with this comment, to the extent it supports transparency and control for consumers. The Agency disagrees in part with this comment, to the extent it argues that the ADMT requirements should be modified. These regulations balance providing privacy protections for consumers with flexibility for businesses to come into compliance.
ADMT	1075	Comment advocates for privacy regulations that enable technology companies to continue providing the essential tools that help businesses connect with and grow their customer base.	The Agency agrees in part with this comment, to the extent it argues that privacy regulations can be supportive of innovation. The Agency disagrees in part with this comment, to the extent it argues that the

			regulations do not support businesses. The regulations balance providing privacy protections for consumers with flexibility for businesses to come into compliance.
ADMT	1087	Comment supports development and use of AI technologies in ways that are human-centric, ethical, and trustworthy, and that mitigate potential risks. Accordingly, regulatory approaches should be technology-neutral and use-case specific, and appropriately focused on technology applications that are truly high-risk.	The Agency agrees in part with this comment, to the extent it supports privacy-protective uses of AI. The Agency disagrees in part with this comment, to the extent it argues that the regulations do not focus on high-risk uses of consumers' personal information. The regulations explicitly address processing that presents significant risk to consumers' privacy or security, and provide rights to opt-out and access ADMT for significant decisions concerning consumers. Additionally, the regulations have been revised to remove references to AI as unnecessary.
ADMT	1104	Comment argues that the proposed restrictions on ADMT and data privacy could impede mortgage approvals and disrupt transactions. Lenders will face challenges if applicants opt-out of ADMT, leading to delays or rejections in loan approvals, potentially causing buyers to miss out on purchasing opportunities.	The Agency disagrees with this comment. The regulations provide consumers with a meaningful opt-out of ADMT while providing flexibility for businesses to come into compliance. With respect to the transactions cited by commenter, the Agency does not believe that the regulations will impede purchasing opportunities. For example, if a business cannot offer an opt-out for loan approvals, it may rely on the human appeal exception.
ADMT	1139	Comment states that the requirements under §§ 7220 and 7222 may lead to conflicting obligations, particularly regarding the right to access ADMT. If certain ADMT outputs are subject to GLBA exemptions, insurers would be forced to provide only partial access to consumers, leading to confusion and frustration.	The Agency disagrees with this comment. The ADMT requirements do not lead to conflicting obligations. If a CCPA exemption applies, the business does not have obligations with respect to the exempted data. If an exemption does not apply and is "personal information" under the CCPA, the business must comply with the relevant CCPA obligations for that personal information. The business must also comply with the ADMT Pre-use Notice and access right with

			respect to personal information subject to the CCPA. In addition, § 7222(*l*) of the regulations is clear that a business may provide additional information to enable a consumer to understand how the ADMT was used to make a significant decision with respect to them. These provisions ensure that consumers receive meaningful information about the relevant ADMT and mitigate the risk of confusion or frustration.
ADMT	1185	Comment argues that the CCPA already regulates biometric data under "sensitive personal information," allowing businesses to use such data for service improvement. The draft rules contradict this by restricting biometric data use in AI improvements. For example, under the draft regulations, a user may opt out of the use of her biometric data to "improve [a business's] algorithm." This is irreconcilable with the statute's express safe harbor allowing businesses to use sensitive personal information to improve the services they offer.	The Agency disagrees with this comment. The CCPA gives consumers many rights, including a right to limit a business's use of sensitive personal information, a right to opt-out of ADMT, and a right to access information about a business's use of ADMT. (*See* Civ. Code §§ 1798.121(a), 1798.185(a)(15).) The ADMT regulations are within the Agency's authority, consistent with the CCPA, and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(15).) However, exercising its discretion, the Agency has revised the definition of ADMT to focus on a higher-risk use of ADMT at this time, which is a use without any human involvement for a significant decision, and removed the training uses of ADMT threshold from Article 11. This balances protections for consumer privacy with simplifying implementation for businesses at this time.
ADMT	1167	Comment argues that the regulations on bias, explainability, and model training may exceed the CPPA's statutory authority under the CCPA. Additionally, pending legislative efforts to regulate AI could lead to overlapping or conflicting laws.	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, it is required to issue

			regulations and impose certain requirements. The regulations are also consistent with the Governor's executive order and other AI frameworks, and similarly take an approach that balances support for businesses with protections for consumers. Nevertheless, exercising its discretion, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time.
ADMT	1207	Comment believes that the proposed rule conflicts with established interpretations of AI regulation, particularly the European GDPR, which focuses only on decisions that significantly affect individuals, rather than the development or training of AI systems. Comment argues that CPPA's proposal improperly extends GDPR concepts beyond their original intent.	The Agency disagrees with this comment. The regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado. The Agency has also revised the regulations to focus on significant decisions to further simplify implementation for businesses at this time. Further, the regulations harmonize with other jurisdictions where possible, but must further the purposes of the CCPA and comply with the requirements for regulations under California law.
ADMT	1212	Comment argues that the Agency's rulemaking process is particularly important given the federal policy shift, including the revocation of a prior Executive Order on AI governance. With federal oversight weakened, California has an opportunity to lead in AI transparency and privacy protections.	The Agency agrees with this comment, to the extent it supports the Agency's rulemaking process.
ADMT	1215	Comment supports transparency requirements for ADMT, particularly for high-risk use cases involving sensitive data or consequential decisions. It agrees with the Agency's risk-based approach, which identifies these contexts explicitly.	The Agency agrees with this comment, to the extent it supports the regulations.

ADMT	1216	Comment supports human intervention as an important way to validate decisions of high consequence of consumers, such as approval for a lower mortgage interest rate, rejection for an auto loan, or flagging someone as suspect in the criminal justice system.	The Agency agrees with this comment, to the extent it supports the human involvement and human appeal provisions in the regulations.
ADMT	1233	Comment argues that the proposed rule should be tailored to address concrete, contextual risks. The proposed rule assumes all ADMT poses risks, failing to differentiate based on the outcome and context in which the technology is used. Regulation should be based on sector-specific and risk-specific approaches, as seen in other regulatory frameworks. Applying the same regulatory requirements to all uses of ADMT, regardless of the context, makes compliance harder and less effective.	The Agency disagrees with the comment. The Agency modified the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. The regulations are meant to be robust and applicable to many factual situations and across industries. The regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope.
ADMT	1246	Comment questions the Agency's authority to regulate certain aspects of ADMT and introduce new statutory definitions, such as "Behavioral Advertising" and "Artificial Intelligence," as these terms do not exist in the CCPA or the CPRA.	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, it is required to issue regulations and impose certain requirements. Nevertheless, exercising its discretion, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references

			to it throughout the regulations to simplify implementation for businesses at this time. The Agency also deleted the profiling for behavioral advertising threshold to simplify implementation for businesses at this time.
ADMT	1276	Comment suggests that AI-driven security tools are critical for detecting zero-day and malware-free attacks by analyzing behavioral patterns instead of known signatures. Allowing individuals to opt out of AI-based cybersecurity could enable adversaries to evade detection.	The Agency agrees with this comment to the extent it supports proactive measures to protect consumers' personal information. The Agency otherwise disagrees with this comment. The Agency has removed the security/fraud-prevention/safety exception from the opt out of ADMT regulations as unnecessary because the Agency modified the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. With respect to AI, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time.
ADMT	1294	Comment emphasizes that AI-driven decision-making in education requires more transparency, review, and recourse. Comment supports the recognition of "extensive profiling" and "significant decisions" in education but recommend expanding the list of decisions that qualify for protection. Comment also calls for clearer standards on when ADMT is "necessary" in education.	The Agency agrees in part with the comment, to the extent it supports transparency and choice regarding businesses' uses of ADMT in the educational context. The Agency disagrees in part with this comment, to the extent it suggests further clarity is needed. The list of decisions in §§ 7001(ddd)(3)(A)-(C), previously §§ 7200(a)(1)(A)(i)-(iii), is appropriate and clear, and no further clarification is needed at this time. With respect to the opt-out exception in § 7221(b)(2),

			previously § 7221(b)(3)(A), the Agency has removed the necessity requirement to simplify implementation for businesses at this time. In addition, the Agency has revised § 7200 to focus on the use of ADMT for significant decisions and revised the definition of ADMT to address a higher-risk use of ADMT without any human involvement.
ADMT	1323	Comment argues that Pre-use Notice requirements, access right, and opt-out for such a broad category of ADMT and training data will have unintended consequences that hurt consumers. Additionally, that restricting training on ADMT systems will have a disproportionate impact on smaller California firms and will harm consumers experience with AI tools.	The Agency disagrees with this comment. The regulations balance providing protections for consumers' privacy while providing flexibility to businesses to come into compliance. In addition, the regulations have been revised to further simplify implementation for businesses at this time, including removing the extensive profiling and training thresholds from Article 11.
ADMT	1333, 1631	Nothing in the statutory text creates an independent ADMT opt-out right. It is limited to existing opt-out rights--sale, sharing, limiting use/disclosure of SPI. The most logical interaction of ADMT with existing opt-out rights is with regard to the processing of SPI to make significant decisions about a particular consumer. This approach is supported by statutory text, which connects the ADMT opt-out right to "profiling." There is also substantial overlap between profiling and SPI concepts. The "profiling" definition has meaningful similarities with the scope of sensitive personal data. To avoid overreaching the statute's authority, the regulations should be limited to the use of ADMT for significant decisions, such as those relating to employment, education, benefits, legal services, and healthcare. If CPPA chooses to remain focused on the nature of the decision, it should narrow the scope of "access to, or provision or denial of, …essential goods and services" to	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT, including profiling. (*See* Civ. Code § 1798.185(a)(15).) The ADMT regulations, both as proposed and revised, are within the Agency's authority and further the intent and purpose of the CCPA. However, the Agency has revised § 7200 to focus on the use of ADMT for significant decisions and revised the definition of ADMT to address the higher-risk use of ADMT without any human involvement. The Agency has also revised the definition of "significant decision" to provide additional clarity and guidance for businesses, and to further simplify implementation for businesses at this time. The revisions to the significant decision definition include removing "access to" and "essential goods or services." The definition is consistent with approaches taken in other

		emergency situations. Comment urges that the scope of § 7200 be limited per § 7150. Extending application to all ADMT uses across the employment lifecycle, including for independent contractors, is overbroad.	jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. To the extent the comment suggests that independent contractors should not have the same privacy protections, the Agency disagrees with this comment. The CCPA specifically includes employees and independent contractors within its scope. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
ADMT	1335, 2017	The regulations invent new obligations, including an opt-out right, for "behavioral advertising." This is inconsistent with the statute and well beyond the scope of the CCPA, where both negotiations with the business community and plain text specifically conceded that businesses could continue to use data from their own customers to improve their products and to advertise to these customers. The CCPA defined the bounds of online advertising regulation to opting out of the "sharing" of personal information for "cross-context behavioral advertising." Moreover, the statute expressly provides that no opt-out right shall apply where the consumer intentionally interacts with the particular business that receives the PI. An opt-out for behavioral advertising would encompass targeted advertising based on consumer's activity "within the business's own distinctly-branded" websites, apps, and services. The Agency cannot unilaterally expand the advertising requirements to an entirely new class of advertising activities and protected speech. Further, the right to opt-out of ADMT used for consumer profiling places a large burden on businesses to entirely redesign their services long used by their own consumers. It would	The Agency disagrees with this comment. The regulations, both as proposed and revised, are within the Agency's authority and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(14)-(15).) They are not unduly burdensome. However, the Agency has revised the regulations to remove the definition of behavioral advertising, and to remove the profiling for behavioral advertising threshold, to simplify implementation for businesses at this time.

		disrupt their ability to do basic first-party advertising to their own consumers.	
ADMT	1336	The Agency's argument that ADMT behavioral advertising opt-out right is analogous to opt-out choices for email and text marketing under other laws, like CAN-SPAM and TCPA, is misplaced. Those laws expressly address consumer choice with respect to the specific manner in which businesses can communicate with the consumer. CCPA does not regulate the communication method, but rather, what information can be used to tailor the content of marketing or advertising materials. Also, CAN-SPAM expressly pre-empts state laws attempting to govern the sending of commercial email.	The Agency disagrees with this comment. However, the Agency has revised the regulations to remove the definition of behavioral advertising to simplify implementation for businesses at this time.
ADMT	1337	The use of PI for first-party advertising is consistent with consumer expectations and consumer benefit from such advertising and marketing. The practical effect of the regulations would be to treat first-party marketing within the context of the consumer's relationship with a data broker. Multiple regulators have recognized that behavioral advertising within the business's own sites, apps, and services does not raise meaningful privacy concerns because such processing is within the context of the consumer's relationship with the business. Stopping first-party ads is not the intention of the CCPA. The ISOR also provides no reasonable basis demonstrating any significant privacy risk or cognizable harm resulting from consumer's PI being process for behavioral marketing.	The Agency disagrees with this comment. However, the Agency has revised the regulations to remove the definition of behavioral advertising to simplify implementation for businesses at this time.
ADMT	1338	Restrictions on first-party marketing raise questions regarding protected speech and would impose significant practical and operational challenges on businesses subject to the CCPA. Even if not subject to	The Agency disagrees with this comment. In addition, the Agency does not believe that the requirements would have violated the First Amendment or would be unduly burdensome. However, the Agency has revised

		strict scrutiny, the test requires that the regulations are not more extensive than necessary to serve a substantial government interest. A broad opt-out right for ADMT behavioral advertising is more extensive than necessary to achieve that interest. Commenter questions what substantial government interest could purportedly be found to support restrictions on behavioral advertising when there is no cognizable harm to a consumer (or device) recognized by a US court that arises from using information already and lawfully collected to place an advertisement intended to be seen by that consumer or device. It also imposes significant costs on businesses through reduced income and increased costs to advertise to new customers.	the regulations to remove the definition of behavioral advertising to simplify implementation for businesses at this time.
ADMT	1366	The regulations should limit ADMT requirements to significant decisions to ensure that they do not restrict California consumers from accessing services they choose to engage with, such as tools to map fitness routes or traffic.	The Agency disagrees with this comment. The ADMT requirements do not restrict consumers from accessing services. They also have been revised to focus on significant decisions to further simplify implementation for businesses at this time.
ADMT	1209	Comment asserts that the proposed opt-out requirement in § 7221 disrupts the distinction between businesses and service providers under the CCPA by placing opt-out responsibilities on AI developers rather than those actually using ADMT. This would make compliance difficult and undermine the CCPA's existing structure. The Pre-use Notice requirements in § 7220 also undermine the clearer and more appropriate obligations on AI developers in other parts of the regulations, such as § 7153.	The Agency disagrees with this comment. The opt-out requirements apply to businesses using ADMT. Service providers must comply with all applicable sections of the CCPA, including providing the same level of privacy protections as required of businesses by the CCPA and these regulations. These are statutory requirements that the regulations implement. With respect to compliance, it is unclear how compliance would be difficult or would undermine the CCPA's obligations for businesses and service providers. The Agency has also taken steps to limit the burden on businesses, including revising the ADMT regulations to focus on the use of ADMT for significant decisions. With respect to the Pre-use

			Notice requirements, they also only apply to businesses using ADMT to make a significant decision, and similarly provide flexibility to businesses in providing the relevant information to consumers. These requirements balance ensuring consumers receive meaningful information to exercise their opt-out and access ADMT rights while providing flexibility to businesses to come into compliance.
ADMT	1356	The regulations create confusing, overlapping requirements for SPI that frustrate the aims of the statute to provide consumers with "meaningful options" for how their SPI is used. Specifically, they would require an opt-out right for training uses of ADMT "capable of" being used for physical or biological identification or profiling, which overlaps with the existing statutory right for consumers to limit the use and disclosure of their sensitive personal information. The statutory text is clear that biometric data reflects physiological, biological, or behavioral characteristics to "establish individual identity," which shares substantial overlap with the proposed "physical or biological identification or profiling" definition. Where a business processes biometric data, it must allow consumers the right to limit, which functionally serves as an opt-out, subject to certain exceptions.	The Agency disagrees with this comment. The regulations do not create confusing or overlapping requirements for sensitive personal information. In addition, the training ADMT threshold has been removed from the opt-out requirements to further simplify implementation for businesses at this time.
ADMT	1362	The CPPA should recognize the benefit to California consumers of research and testing of ADMT and ensure the exclusion of those uses from prescriptive regulations. The regulations should not hamper other internal testing activities by the business to the benefit of consumers, such as self-testing to identify, mitigate, or prevent discrimination or otherwise ensure compliance with the law. The right to limit provides the	The Agency disagrees with this comment. The regulations do not hinder internal testing activities. In addition, the Agency has revised § 7200 to focus on the use of ADMT for significant decisions, and revised the definition of ADMT to focus on a higher-risk use of ADMT at this time, which is a use without any human involvement.

		same exception. Businesses need not post a notice of right to limit if it processes SPI "[t]o verify or maintain the quality or safety of" or "improve, upgrade, or enhance" a service or device that is "owned, manufactured by, manufactured for, or controlled by the business." Accordingly, any ADMT opt-out right or related obligation should not apply when ADMT is used for such purposes. The value of internal research and testing has been widely recognized by the NIST AI Risk Management Framework, the Colorado AI Act, and other regulators.	
ADMT	1492	Comment suggests the Agency specifying that the requirements of this Article do not apply to the use of ADMT in motor vehicles. Federal agencies like the National Highway Traffic Safety Administration are the appropriate authority to regulate vehicles and vehicle systems using ADMT as they currently establish, monitor, and enforce vehicle safety regulations.	The Agency disagrees with this comment. To the extent a business is using ADMT for a significant decision, it is subject to the requirements of Article 11. An exemption for motor vehicles is not necessary and would not further protect consumer privacy.
ADMT	1503	Comment suggests that the regulations should be updated to prohibit ADMT systems that rely on emotion detection technology, that involve government use of facial recognition technology, or for predictive policing or in child-welfare proceedings. However, if those prohibitions are not added, then the regulations should at least categorically require that an opt-out be provided to consumers.	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations governing opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a).) With respect to the opt-out, a business that uses the technologies cited by commenter as ADMT to make a significant decision about a consumer must comply with the opt-out requirements. A business also may rely on the human appeal exception. Prohibiting these technologies is not necessary at this time.
ADMT	1505	Comment suggests that the regulations should specify objective accuracy or performance benchmarks for ADMT systems to avoid businesses declaring flawed	The Agency disagrees with this comment. The regulations provide a performance-based standard that is adaptable to many use cases and contexts.

		systems as "working as intended" without accountability.	Additional requirements are not necessary at this time.
ADMT	1520, 1521	Comment argues that uses of AI for verifying test taker identity via photographic matching and for monitoring testing sessions via video/audio do not constitute high-risk AI activities. These methods preserve test integrity without involving biometric templates or invasive profiling. Comment also argues that traditional automated scoring of multiple-choice answers using optical/computer-based systems does not constitute AI or ADMT under the regulations. These systems operate based on human-created rubrics and do not process personal information, and therefore should not be subject to regulation as "high-risk" AI. Similarly, automated scoring of written answers should not be classified as AI or high-risk ADMT. These systems also rely on human-developed rubrics and do not use personal information.	The Agency disagrees with this comment. The use of ADMT to make a significant decision about a consumer, including certain education decisions, presents significant risk to consumers' privacy. Whether the specific ADMT identified by the comment are subject to Article 11 is a fact-specific analysis. In addition, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time.
ADMT	1526, 1530, 1532, 1663, 1665, 1666, 1667, 1668	The ADMT rules should not override existing FCRA and GLBA exemptions. Maintaining these exemptions is essential to enable timely housing decisions and effective fraud prevention in rental housing. Many uses of ADMT in rental housing, such as for screening, identity verification, or fraud detection, are already regulated by FCRA and GLBA and exempt from the CCPA and the ADMT regulations. Comment requests clarifying that ADMT rules do not apply to data subject to GLBA, CFIPA, or FCRA. The Agency should clarify that the ADMT regulations do not apply to FCRA and GLBA/CFIPA data and exclude decisions involving GLBA/CFIPA and FCRA data from the examples in the term "significant decision." Financial institutions should be exempted from the ADMT regulations due to existing	The Agency disagrees with this comment. The CCPA includes data-level exemptions, including for information subject to the Gramm-Leach-Bliley Act and implementing regulations and for information governed by HIPAA; but it applies to "businesses," is intended to supplement federal and state law, and does not exempt financial institutions. (*See* Civ. Code §§ 1798.140(d), 1798.145(c)(1), (e), 1798.196.) The CCPA directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. Finally, the ADMT regulations

		regulatory frameworks already governing their use of GLBA/CFIPA/FCRA data and ADMTs. These include anti-discrimination laws (ECOA), data accuracy/disclosure mandates (FCRA), privacy protections (GLBA/CFIPA), fair business practice enforcement (UDAAP/UDAP, UCL), and agency-issued AI/ADMT guidance. Existing federal laws (ECOA and FCRA) already require specific disclosures for adverse actions in lending decisions. Imposing the ADMT requirements in the same space would be duplicative, unnecessary, and would create regulatory conflict.	have also been revised to further simplify implementation for businesses at this time.
ADMT	1536	Comment asserts that the ADMT-related notice and opt-out provisions in the draft rules are too broad, treating low-risk uses of AI the same as high-risk decisions. They caution that excessive notifications could harm user experience and disproportionately burden small businesses that rely on e-commerce.	The Agency disagrees with this comment. The regulations are not overly broad. Nevertheless, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time. The Agency also modified the ADMT regulations to focus on the use of ADMT for significant decisions to simplify implementation at this time, and accordingly revised the exceptions to when a business must provide an opt-out from its use of ADMT. The Agency also revised the Pre-use Notice requirements, to provide businesses with flexibility in how they consolidate or include them with the Notice at Collection, and to simplify implementation at this time. Additionally, the Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Moreover, most of the costs of the regulations fall on larger businesses dealing with a large amount of personal information and with

DRAFT

			annual revenues that are greater than $28 million. Nevertheless, the Agency has modified the regulations to significantly reduce their costs on small businesses.
ADMT	1588, 1920, 1923, 1924, 1950	The proposed regulations require opt-outs even if a human assists with the decision, then offers a limited reprieve from that opt-out if there's an appeal mechanism, which creates a regulatory burden while offering no privacy benefit. If a human is materially involved in a decision, no opt-out should be required from the outset. This would cut down on needless paperwork. Even though CCPA's ADMT language is derived directly from GDPR Article 22, it differs from GDPR's law, which only restricts solely automated decisions with legal impacts. It also differs from Colorado's privacy law, which excludes human-involved decisions from opt-outs. The Agency should focus on significant, fully automated decisions where consumers are denied something significant — then they should have the right to opt out and understand the decision-making algorithm. This would ensure that the proposed regulations are narrowly tailored to govern only access and opt-out rights. The regulations should be aligned with other emerging frameworks on ADMT and exclude low-risk, low-complexity and socially beneficial technologies. Systems performing narrow procedural tasks should be exempted, and the list of presumptive technological exceptions should be expanded to include systems used for cybersecurity purposes.	To the extent the comment suggests that the CCPA uses GDPR's Article 22 language or is limited to "solely automated decisions," the Agency disagrees. CCPA's delegation to the Agency regarding ADMT is not limited to "solely" automated decisionmaking. Rather, the CCPA directs the Agency to issue regulations governing access and opt-out rights "with respect to a business' use of automated decisionmaking technology, including profiling." (*See* Civ. Code § 1798.185(a)(15).) The ADMT regulations are within the Agency's authority and further the intent and purpose of the CCPA. Nevertheless, the Agency modified the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and § 7200, to focus on the use of ADMT for significant decisions to simplify implementation at this time. As revised, the regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. With respect to the human appeal exception, the regulations balance privacy protections for consumers and flexibility for businesses regarding how to address consumers' concerns about the use of ADMT to make significant decisions about them. However, the Agency revised

			the human-appeal exception to clarify what a business must do to qualify for the human appeal exception. The exception includes requirements such as the human reviewer considering the information the consumer provided in support of their appeal, knowing how to interpret and use the output of the ADMT, and having the authority to change the significant decision based upon their analysis. The Agency will continue to monitor the marketplace to determine whether modifications to the regulations are necessary.
ADMT	1589	Comment suggests the Agency recognizing that meaningful ADMT transparency is contextual. Regulations governing ADMT system logic and likely outcomes should be flexible enough to accommodate different contexts without requiring businesses to disclose trade secrets or intellectual property.	The Agency disagrees with this comment, to the extent it argues that the regulations are not flexible. The regulations for Pre-use Notices and the right to access ADMT provide clarity to businesses about their obligations, while being adaptable to a variety of use cases and contexts. In addition, the regulations have also been revised to clarity that when a business provides the required information for a Pre-use Notice and a response to an access request, it is not required to disclose trade secrets.
ADMT	1590	Comment recommends employing contextual, use-based evaluations to promote ADMT accuracy and the implementation of appropriate non-discrimination safeguards.	The Agency agrees in part with this comment, to the extent it supports ADMT accuracy and non-discrimination. The Agency disagrees in part with this comment, to the extent it argues that the regulations need to be modified. The regulations provide a flexible, performance-based standard for businesses with respect to accuracy and non-discrimination that is adaptable to a variety of use cases and contexts.
ADMT	1605	Comment states that the CCPA only narrowly authorizes the Agency to regulate access and opt-out rights concerning businesses' use of ADMT and profiling, as per § 1798.185(a)(15). They argue that this provision	The Agency disagrees with this comment. The ADMT regulations are within the Agency's authority and further the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations governing

		does not authorize the Agency to regulate all aspects of ADMT and profiling more broadly, since personal information processing is already governed under existing CCPA provisions. Comment argues that the regulations cast too broad a net for ADMT usage and should instead focus on processing that is solely automated and has legal or similarly significant effects. They note that § 7200(a)(3) erroneously includes "training" uses of ADMT, which contradicts the definition in § 7001(f), since training does not constitute decisionmaking and does not impact consumer privacy directly.	access and opt-out rights with respect to businesses' use of ADMT but does not define ADMT. (*See* Civ. Code § 1798.185(a).) However, exercising its discretion, the Agency has revised the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. This includes removing the training ADMT threshold from the ADMT regulations. The regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope.
ADMT	1674	The Agency has clear authority to promulgate rulemaking on ADMT.	The Agency agrees with this comment and notes commenter's support.
ADMT	1675	The ADMT regulations are in line with what other states (e.g., Colorado) are doing to regulate ADMT. The proposed regulations will not impose unreasonable or unique burdens on companies, but would provide clarity and assurance to CA consumers and workers that their rights are protected.	The Agency agrees with this comment and notes commenter's support.
ADMT	1676	Regulating ADMT is necessary to protect Californians because commercial surveillance of consumers is out of control. Commercial surveillance systems enable companies to collect and commodify every bit of consumers' personal data, including sensitive personal information. The use of ADMTs in significant decisions threatens discriminatory outcomes across multiple	The Agency agrees with this comment, to the extent it supports the privacy protections in the regulations.

		industries (i.e., healthcare, education, employment, financial services, and public benefits). Commenter provides multiple examples of algorithmic discrimination and unfair decisionmaking in ADMTs.	
ADMT	1677	Regulating ADMT is necessary because behavioral advertising invades consumer privacy. Behavioral advertising allows advertisers to determine who should be targeted with economic opportunities based on detailed profiles of individuals. This can cause harm to marginalized communities by reinforcing inequities in opportunities for housing, healthcare, financial services, employment, and educational opportunities. Commenter provides examples.	The Agency agrees in part with this comment, to the extent it supports providing privacy protections to consumers in the behavioral advertising context. The Agency has revised the regulations to remove the profiling for behavioral advertising threshold, to further simplify implementation for businesses at this time.
ADMT	1678	Regulating ADMT is necessary because Americans are dissatisfied with how AI programs make decisions about their lives. Consumers are often left unable to determine how ADMT outputs made decisions about them, what data was collected, for what reason, how it was used, and how to appeal such a decision. Because ADMTs can centralize biased data and assumptions and automate the decision-making process, they expand the scale of erroneous and unfair outcomes, including discrimination, to masses of people. Consumers should have actionable transparency and meaningful choices around ADMTs, including those used in behavioral advertising.	The Agency agrees with this comment, to the extent it supports the ADMT protections provided in the regulations. The Agency has removed the ADMT thresholds regarding extensive profiling and training uses of ADMT to further simplify implementation for businesses at this time.
ADMT	1680, 1966	The ADMT provisions should retain the right of consumers to opt out of profiling for behavioral advertising. Due to the risks that profiling of consumers poses to their privacy, short of banning behavioral advertising outright, allowing individual to opt-out of the use of ADMTs for behavioral advertising purposes, with no exemptions, is the best way to protect Californians.	The Agency agrees with this comment to the extent that it supports further protections for consumers' privacy. However, the Agency has revised the regulations to remove the definition of behavioral advertising, and to remove the profiling for behavioral

		The opt-out provides consumers with choice and encourages the advertising industry to innovate toward advertising methods that do not sacrifice consumer privacy. This opt-out is significant because it addresses large consumer-facing platforms that serve behavioral advertising.	advertising threshold, to simplify implementation for businesses at this time.
ADMT	1681	Commenter commends the Agency for including that the consumer can prevent the use of their data for training ADMT systems that are capable of being used for a significant decision, to establish individual identity, for physical or biological identification or provision, or for generation of a deepfake. Californians should have a say in whether they consent to their personal data being used to train ADMTs, separate from their choice to interact with the covered entity in the first place.	The Agency agrees with this comment to the extent that it supports further protections for consumers' privacy. The Agency has removed training uses of ADMT from the requirements to further simplify implementation for businesses at this time.
ADMT	1682	The Agency should extend consumers' right to opt-out of the use of personal data to train AI to include generative AI. Such a use presents a significant risk to consumer's privacy under § 7150(b). If the use triggers a risk assessment, consumers should be given a training opt-out. This kind of use is unnecessary, unexpected, and out-of-context. It can also lead to the model leaking personal data unexpectedly when it is deployed to the market.	The Agency agrees with this comment to the extent it supports further protections for consumers' privacy. The Agency has removed training uses of ADMT from the requirements to further simplify implementation for businesses at this time.
ADMT	1684, 1750	Comment expresses support for the Agency's efforts to regulate ADMT. Commenter commends the Agency for including Pre-use Notice requirements for businesses that use ADMTs and the right for consumers to access ADMTs. ADMTs are currently opaque to consumers that interact with them, preventing access to inner workings of how decisions were made. This opacity prevents broader understanding of how ADMTs impact consumers based on protected classes, undermining	The Agency agrees with this comment, to the extent the commenter is expressing support for the regulations.

		meritorious antidiscrimination and consumer protection claims. The regulations are viewed as an important step to rebalance the current informational asymmetry between consumers and businesses.	
ADMT	1686, 1969	Comment recommends clarifying how the right of correction must work in practice. There is no clear mechanism for remedying decisions made about them based on inaccurate information fed to an ADMT. The Agency should clarify either that (1) the right to correct information fed into an ADMT inherently includes a right to have the decision reconsidered, or (2) individuals have a separate right to reconsideration when decisions made using an ADMT were based on inaccurate information. This is already in the Colorado AI Act.	The Agency disagrees with this comment. Consumers have a right to correct under the CCPA, and businesses must inform consumers of their CCPA rights and how to exercise them when responding to an access ADMT request. This provides clarity on how consumers can correct inaccurate personal information about them that has been used to make a significant decision. Commenter's suggestions are not necessary because the regulations are both clear and provide the appropriate mechanism for correcting inaccurate information.
ADMT	1705, 1707, 1713, 1839, 1907	Comment objects to regulating technologies that "substantially facilitate" human decisionmaking, including tools like spreadsheets used for analysis. Comment argues that plain text of the statute is clear and unambiguous that the regulations are limited to solely automated decisionmaking technologies. Comment advocates for alignment with laws in other jurisdictions to reduce confusion, like GDPR, which apply only to decisions made solely by automated means. This would enhance consumer protections while making compliance with the proposed rules less burdensome. Comment argues that the regulations are overly rigid and burdensome, imposing EU-style obligations without clear consumer benefit. They suggest aligning the rules with global privacy norms and statutory limits under the CCPA, focusing only on consequential uses of ADMT. They recommend narrowing the scope of ADMT obligations to reduce	The Agency disagrees with the comment. The regulations are within the Agency's authority and consistent with the CCPA's plain text and purpose. The Agency also modified the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and revised § 7200 to focus on the use of ADMT for significant decisions to simplify implementation at this time. The regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope.

		compliance burdens and legal uncertainty, which might otherwise drive businesses away from offering services. One comment recommends revising the section as follows: A business that uses automated decisionmaking technology as the sole basis for making a significant decision concerning a consumer must comply with the requirements of this Article.	
ADMT	1752	Comment argues that § 7221 is insufficient unless it also requires businesses to explain the consequences of opting out. Without this clarity, consumers may hesitate to exercise their rights due to uncertainty about what will happen next.	The Agency agrees with this comment in part and has revised § 7220(c) to require businesses to disclose to consumers how the significant decision would be made if a consumer opts out.
ADMT	1755, 1756, 1910	Comment supports the Agency's efforts to regulate ADMT, however, comment emphasizes that more must be done for meaningful protections. Comment suggests that ADMTs must be monitored on an ongoing basis to ensure that they are not deviating from the human decisionmaking processes they are supposed to be emulating. This would help identify discriminatory patterns and ensure fair treatment of those who opt out. The Agency should also provide guidance concerning what non-ADMT alternatives a company can or must offer consumers that opt out. Comment also states that post-decision explanations must be detailed and put in relevant context in order to be useful to consumers. In addition to § 7222's requirements under (b)(4), businesses should also be required to disclose what personal information was most relevant to the key factors articulated in § 7222 (b)(4)(B), what the sources of that personal information were, and how that personal information interacted with the key factors. Comment argues that businesses should be required to provide information specified under § 7222 (b)(4)(C) ("A	The Agency agrees with the comment to the extent that it supports protections for consumers' privacy. However, the Agency modified the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and § 7200, to focus on the use of ADMT for significant decisions to simplify implementation at this time. The regulations already include clarity and guidance for businesses and protections for consumers' privacy, including requirements that a business conduct a risk assessment when it plans to use ADMT for a significant decision concerning a consumer. This includes identifying and documenting safeguards to address negative impacts to consumers, which may include implementing policies, procedures, and training to ensure that the ADMT works for the business's purpose and does not unlawfully

		business also may provide the range of possible outputs or aggregate output statistics to help a consumer understand how they compare to other consumers"). Comment also lists reasons why additional requirements for ADMT implementers is needed, such as the ADMT products' tendency of reinforcing existing biases, errors in ADMT outputs, the lack of ethical judgment that human decisionmakers can bring etc.	discriminate. (*See* § 7152(a)(6)(A)(iv).) The ADMT regulations balance protections for consumers' privacy and providing businesses with flexibility. Further, the Agency does not believe commenter's recommendations are necessary at this time. Under the revised regulations, a business must disclose information about the logic of the ADMT, which must enable the consumer to understand how the ADMT processed their personal information to generate an output with respect to them. The revised regulations ensure that consumers understand how their personal information was processed by the ADMT, which can include the types of information requested by commenter.
ADMT	1757	In order to increase the likelihood that the post-decision explanations businesses generate are both plain language and sufficiently detailed, comment recommends the Agency provide an appendix with examples of hypothetical explanations that meet the Agency's expectations.	The Agency disagrees with this comment. The regulations provide clarity and guidance regarding what information must be provided to a consumer in response to an access ADMT request. The Agency has determined that no further clarification is needed at this time.
ADMT	1758	Comment supports the development of AI and favors narrowly tailored notice, opt-out, and transparency rules. It endorses a voluntary, risk-based framework, such as the NIST AI Risk Management Framework. It urges the Agency to ensure that its proposed rules do not extend beyond the specific mandates of the CCPA, or conflict with existing requirements.	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purpose of the CCPA. The CCPA directs the Agency to require businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment and submitted it to the Agency on a regular basis. (Civ. Code § 1798.185(a)(14).) The CCPA further directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(14)–(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent

			with the CCPA; thus, it is required to issue regulations and impose certain requirements. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. Nevertheless, exercising its discretion, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time. With respect to the ADMT framework, the Agency modified the definition of ADMT to focus on a higher-risk use of ADMT at this time, which is a use without any human involvement; and revised the definition of significant decision and § 7200, to focus on the use of ADMT for significant decisions to simplify implementation at this time. As revised, the regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. Finally, with respect to risk assessment requirements, the Agency revised the regulations to simplify implementation at this time, including removing requirements regarding actions to maintain the quality of personal information and clarifying the types of safeguards businesses must identify and that the safeguards listed are examples. (*See* §§ 7152(a)(2), (6).)
ADMT	1759	Comment suggests that the Agency should narrow its approach to regulating ADMTs to ensure that it targets only the highest-risk uses of ADMTs for decisions concerning individuals, and does not stifle innovation by creating unnecessary regulatory duties and obligations, particularly for small- and medium-sized businesses.	The Agency disagrees with the comment. The Agency modified the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and §

			7200, to focus on the use of ADMT for significant decisions to simplify implementation at this time. Respecting consumer privacy and data protection is not contrary to innovation and entrepreneurship; rather, the regulations foster the development of privacy-by-design products and services. The Agency has appropriately considered the impact on businesses and innovation, and has made efforts to limit the burden of the regulations while implementing the CCPA. The regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Moreover, most of the costs of the regulations fall on larger businesses dealing with a large amount of personal information and with annual revenues that are greater than $28 million. Nevertheless, the Agency modified the regulations to significantly reduce their costs on small businesses.
ADMT	1767	Comment believes that these obligations may be well intentioned, but given the inherent complexity of the technology at issue, and the underlying machine learning systems, these disclosures are not likely to provide meaningful or actionable information to consumers. Instead, disclosures like this may increase consumer notice fatigue, or confuse consumers who may not understand the underlying technology supporting these systems.	The Agency disagrees with the comment. However, the Agency modified the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and § 7200, to focus on the use of ADMT for significant decisions to simplify implementation at this time. With respect to the disclosure requirements, Pre-use Notices are necessary to ensure that consumers have relevant information about use the of ADMT to meaningfully exercise their CCPA rights. It is unlikely that consumers will have notice fatigue from the Pre-use Notice, as it is only required in limited circumstances,

			and businesses have flexibility in providing the Pre-use Notice as part of a Notice at Collection, which reduces concerns about overwhelming consumers with notices. The CCPA provides consumers with the right to access ADMT and explicitly requires that a business's response to access requests include meaningful information about the logic involved in those decisionmaking processes, as well as a description of the likely outcome of the process, with respect to the consumer. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Nevertheless, the Agency has revised the regulations to provide further clarity about what type of information may be provided to a consumer to meet the CCPA's requirements and to simplify implementation for businesses at this time. The access right requirements ensure that consumers receive meaningful information in a way that is easy to understand. The Agency does not believe that these requirements will lead to notice fatigue or confusion.
ADMT	1796, 1798, 1799	Comment argues that there is no CCPA provision requiring businesses to respond to consumer's questions. As a result, questions are ignored or deflected to vague privacy policies. Consumers often receive generic acknowledgments instead of specific responses to their CCPA rights requests from businesses. Requests to access ADMT, requests to appeal ADMT, and requests to opt-out of ADMT are meaningless without an inventory of all decisions a company makes about consumers, regardless of the technology or person used to make those decisions. Comment also states that, as a consumer, decisions and actions the commenter makes will impact the	The Agency disagrees with this comment to the extent that it suggests that the Agency should modify its regulations. With respect to disclosures and access rights, existing regulations provide consumers with information. (*See, e.g.*, Article 2, § 7024.) The proposed regulations ensure that consumers have meaningful information about use the of ADMT with respect to them when they are exercising their CCPA rights and when they request access to ADMT. (*See* §§ 7220, 7222.) They also provide a flexible, performance-based standard for businesses regarding how to provide the required information. The regulations also include requirements to enable consumers to opt-out

		regulations at some point. Therefore, comment outlines 12 specific "special needs" that are not explicitly included in the regulations, such as knowing what they are opting out of, verifying fulfillment, communicating directly with businesses, knowing data sharing and processing details, and having validation and incentives. While the regulations cover many of these, comment believes that the lack of case law or enforcement mechanisms present challenges.	of ADMT. (*See* § 7221.) The commenter's suggestion is no more effective or appropriate than those adopted by the Agency.
ADMT	1804	Comment argues that consumers want transparency on how ADMT impacts them, including insight into the entire supply chain and decisions made by organizations. Comment requests that the Agency conduct and publish the mandatory risk assessment (PTA, PIA, SIMM) required by all agencies in the State of California as an appendix to the ADMT risk assessment as mandated under these draft Regulations.	The Agency disagrees with this comment. The commenter's suggestion is no more effective or appropriate than those adopted by the Agency. The information the commenter suggests be published would not provide information to consumers about a business's use of ADMT or consumers' rights to opt out of ADMT or to access ADMT.
ADMT	1808	Comment advocates for the ability to use AI-driven tools as an Authorized Agent to manage and control their personal data.	The Agency disagrees with this comment to the extent that it suggests that the Agency should modify the regulations. The regulations do not prescribe the tools that authorized agents use to manage or control their personal data. The commenter's suggestion is no more effective or appropriate than those adopted by the Agency.
ADMT	1844, 1865	Comment argues that the proposed definitions of "significant decision" and "automated decisionmaking technology" are too expansive and should be narrowed. The definition of ADMT would cover virtually all software, and extends beyond the statute's scope. Many uses of automated technology are beneficial to consumers with only negligible impacts on privacy. In addition, the regulations extend beyond traditional privacy concerns, implicating attenuated issues like	The Agency disagrees with the comment. The ADMT regulations are within the Agency's authority and further the intent and purpose of the CCPA. The CCPA directs the Agency to issue regulations governing access and opt-out rights with respect to businesses' use of ADMT but does not define ADMT. (*See* Civ. Code § 1798.185(a).) However, the Agency modified the definition of ADMT to focus on a higher-risk use of ADMT at this time, which is a use without any human

		discrimination and disparate impact. Comment also points out that the basic, day-to-day functions use of technology for an app-based platform is not a "significant decision."	involvement. This balances protections for consumer privacy and simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and § 7200, to focus on the use of ADMT for significant decisions to simplify implementation for businesses at this time. Lastly, the Agency has explained how discrimination on the basis of protected characteristics is a privacy harm.
ADMT	1874	Comment believes that the proposed regulations carry significant risks for innovation and U.S. technological competitiveness, with California standing to lose the most. Excessive regulations consistently reduce innovation by increasing costs and discouraging risk taking by entrepreneurs and businesses alike.	The Agency disagrees with this comment. Respecting consumer privacy and data protection is not contrary to innovation and technological competitiveness; rather, the regulations foster the development of privacy-by-design products and services. Nevertheless, the Agency has modified the regulations to significantly reduce the costs of the regulations.
ADMT	1911	Comment states that the Agency appropriately exercised its statutory authority to issue the proposed ADMT regulations. This broad delegation has been repeatedly recognized and endorsed by state appellate courts. Furthermore, the Legislature specifically charged the Agency with issuing "regulations governing access and opt-out rights with respect to a business' use of automated decisionmaking technology." In addition, in 2024, California amended the CCPA to clarify that "personal information" includes physical, digital, and abstract digital formats — such as metadata and AI systems capable of outputting personal information. Since many ADMTs rely on personal information to make decisions, their proliferation is a "change in technology" that justifies regulatory updates.	The Agency agrees with this comment and notes commenter's support.

ADMT	1922	The Agency should remove or clarify "access to and provision of" goods and services to reduce unnecessary opt-outs.	The Agency agrees with this comment in part and has revised the definition of "significant decision." The revisions include removing "access to" and "essential goods or services." As revised, the definition is consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope.
ADMT	1944, 1962	The regulations fail to recognize that data-powered and automated data tools offer many benefits. Targeted ads help consumers find products and services they really need and help small businesses compete against bigger players. Comment asserts that the regulations put first-party advertising in the same category as high-impact ADM. This shift in California law will create problems for businesses and consumers.	The Agency disagrees with this comment. However, the Agency has revised the regulations to remove the definition of behavioral advertising, and to remove the profiling for behavioral advertising threshold, to simplify implementation for businesses at this time.
ADMT	1964	Comment opposes industry position and states that the Agency has clear legal authority to regulate ADMT. The use of ADMTs in significant decisions is a harmful part of the commercial surveillance ecosystem that can reproduce discriminatory outcomes.	The Agency agrees with this comment to the extent that it supports the regulations.
ADMT	1967	The consumer's right to opt-out should be extended to use of personal data to train generative AI.	The Agency agrees with this comment to the extent that it supports further protections for consumers' privacy. However, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time.
ADMT	1986, 1987	The Agency should require purpose limitation for ADMT. Data should be collected only for specific, explicit, and legitimate purposes. Personal information collected for	The Agency disagrees with this comment's suggestion to modify the regulations, because the CCPA and existing regulations already restrict businesses'

		one purpose, such as loan decisions, could not be repurposed for another, like employment decisions without explicit consumer consent. The Agency should implement data minimization standards. Businesses should collect only the minimum amount of data necessary for the intended purpose. Sensitive data, such as health records, should not be used by ADMT unless relevant and legally permissible. As required in the European Data Protection Board's December 2024 guideline, AI systems must establish legitimate interest and conduct necessity tests to protect individual rights.	collection and use of personal information. (*See* Civ. Code § 1798.100(c), § 7002.) With respect to AI, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time.
ADMT	1988	The Agency should mandate privacy enhancing techniques, AKA PET's. The CCPA should require businesses to adopt PETs such as data and automatization and encryption to minimize the risk of unauthorized access and data misuse. It should also ensure PET requirements apply to all entities within the ADMT ecosystem, including third-party providers.	The Agency agrees with this comment to the extent that it supports protecting consumers' personal information. However, the Agency disagrees with this comment's suggestion to mandate PETs at this time. The comment's suggestion is not more effective or appropriate than the regulations adopted by the Agency. The Agency will continue to monitor the marketplace as practices evolve, to determine whether modifications to the regulations are necessary.
ADMT	1998	Employers face excessive restrictions on ADMT use in hiring, promotions and compensation decisions, which could hinder business operations.	The Agency disagrees with this comment. The CCPA explicitly provides privacy protections to employees and independent contractors, and provides consumers with rights to access and opt-out of ADMT. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. Nevertheless, the Agency modified the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of

			significant decision and § 7200, to focus on the use of ADMT for significant decisions to simplify implementation at this time.
ADMT	2002	The regulations are insufficiently risk based and depart from established global privacy frameworks and standards. The regulations go far beyond the Agency's express statutory authority and beyond the scope of privacy regulations and veer into general regulations of ADMT and AI technology when voters, in fact, only granted very specific and narrow authority for rules governing access and opt-out rights with respect to business use of ADMT.	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(14)-(15).) Nevertheless, the Agency modified the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and § 7200, to focus on the use of ADMT for significant decisions to simplify implementation at this time. As revised, the regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. Lastly, exercising its discretion, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time.
ADMT	2022	The regulations, especially those concerning ADMT, could frustrate consumers and hinder their online experiences, harming small and local businesses in particular that rely heavily on e-commerce.	The Agency disagrees with the comment. The Agency modified the definition of ADMT to focus on a higher-risk use of ADMT at this time, which is a use without any human involvement. Separately, the Agency revised the definition of significant decision and § 7200, to focus on the use of ADMT for significant decisions. These revisions include removing the profiling for behavioral advertising threshold. The

			proposed regulations balance protections for consumer privacy and simplifying implementation for businesses at this time.
ADMT	2023	Simplifying notice requirements to focus on high-risk activities would benefit both consumer privacy and business efficiency. By treating low-risk AI applications similarly to high-stakes decisions, the regulations discourage technologies that could enhance efficiency, productivity, and growth across various sectors.	The Agency disagrees with the comment. Nevertheless, the Agency modified the definition of 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 simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision and § 7200, to focus on the use of ADMT for significant decisions to simplify implementation at this time. In addition, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time. Lastly, respecting consumer privacy and data protection is not contrary to innovation and entrepreneurship; rather, the regulations foster the development of privacy-by-design products and services. The Agency has appropriately considered the impact on businesses and innovation.
ADMT	2031	Commenter supports the adoption of these regulations. The Agency has the authority and the duty under the CCPA to adopt a strong regulatory framework to protect both workers and consumers from privacy harm that can result from the collection and use of their data through algorithmic technologies. In healthcare settings, ADMT's have been demonstrably prone to serious inaccuracies and biases, and without the Agency's rules, healthcare decisions and staffing issues are being made by opaque ADMT and other algorithmic	The Agency agrees with this comment and notes commenter's support.

		decisionmaking systems. Adoption of these regulations is necessary to protect worker data privacy and to protect against harmful use of worker data by employers. These regulations establish basic requirements on worker and consumer notice and access to ADMT's and other data driven tools.	
ADMT	2034	In personalized medicine, ADMT is used to analyze complex data and recommend treatments. ADMT is speeding up the drug discovery process, bringing new medical therapies to market faster for patient treatment. It is also used to identify patients to diversify clinical trials and to reduce the lengthy paperwork process allowing scientists to focus on the science. The regulations need to be revised to be consistent with the existing statutory opt-out rights. It should be limited to significant decisions made without human involvement that present a significant risk to consumer privacy.	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The regulations are consistent with the CCPA and with other privacy frameworks. The also Agency revised the definition of ADMT to focus on a higher-risk use of ADMT at this time, which is a use without any human involvement. Further, the Agency revised the definition of significant decision and revised § 7200 to focus on the use of ADMT for a significant decision, to simplify implementation for businesses at this time.
ADMT	2035, 2036	Comment states that artists are consumers of software programs, applications, and cloud storage that they must use as employees. They must also advertise on websites to get work. These products steal artists' data and then compete against them in the marketplace. Gen-AI is trained on work stolen from artists without their consent, credit, or compensation. The artist community needs government to right this wrong. That way creatives and their livelihoods can peacefully coexist with new AI technologies and will not get left behind. The only practical way to legitimately achieve opting out from having their data taken is through a robust and informative pre-use, opt-out notification	The Agency agrees with this comment to the extent it supports safeguards for consumers' privacy as businesses use ADMT. Nevertheless, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time. The Agency also revised the definition of ADMT to focus on a higher-risk use of ADMT at this time, which is a use without any human involvement. The Agency has also revised the uses of ADMT that require a business to comply with Article 11's requirements to focus on

		system, which these proposed regulations recommend. We support the proposed direction these regulations are taking.	the use of ADMT for significant decisions to simplify implementation at this time.
ADMT	2043, 2044	Comment states that voice actors need consent, control, and compensation for the use of their voices, or biometric data. There should be an optout prior to the ingestion of their voice and consumers should have the ability to remove their voice before its used to train a model or to become a clone and be used either against us or replace us in some capacity. We need laws that protect our likeness and image and laws that give the right of publicity to all people across the nation and around the world.	The Agency agrees with this comment to the extent it supports safeguards for consumers' privacy as businesses use ADMT. However, the Agency deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation at this time. The Agency has also revised the definition of ADMT to focus on a higher-risk use of ADMT at this time, which is a use without any human involvement. The Agency has also revised the uses of ADMT that require a business to comply with Article 11's requirements to focus on the use of ADMT for significant decisions to simplify implementation at this time.
ADMT	2046, 2047, 2048, 2049	Comment argues ADMT have been developed and deployed in a vacuum of regulation, allowing businesses to self-regulate and mask discriminatory and harmful data collection and use practices. Proposed rules should not allow companies to self-regulate and opt their ADMT out of application of regulations. Comment argues the use of insufficiently tested and regulated technologies in health care settings threatens patient care and safety. Protecting patient privacy protects independent exercise of clinical judgment and prevents deskilling of health care professionals. Particularly given the life-or-death implications of health care settings, consent should be informed, opt-in, and the Agency should not consider profit from data as a legitimate business benefit. Comment argues the health care industry has already automated data collection in a	The Agency agrees with this comment to the extent it supports safeguards for consumers' privacy as businesses use ADMT. However, the Agency has deleted the definition of artificial intelligence as unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time. The Agency has also revised the definition of ADMT to focus on a higher-risk use of ADMT at this time, which is a use without any human involvement. The Agency has also revised the uses of ADMT that require a business to comply with Article 11's requirements to focus on the use of ADMT for significant decisions to simplify implementation at this time. Comment's recommendations are not necessary at this time. The CCPA directs the Agency to issue regulations

		diverse array of functions. These technologies can be part of a complex surveillance network of workers and patients and often involve gathering biometric data. Comment argues generative AI and LLM systems are often trained by other AI or rely on serious inaccuracies, biases, or flawed data resulting in inappropriate or harmful patient care recommendations.	governing opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The regulations also require businesses that process consumers' sensitive personal information or use ADMT for a significant decision to conduct a risk assessment. (*See* § 7150(b)(2).) Further, existing regulations already restrict businesses' collection and use of personal information. (*See* § 7002.) Finally, the CCPA includes data-level exemptions, including for information governed by HIPAA and the CMIA, but it applies to "businesses." (*See* Civ. Code §§ 1798.140(d), 1798.145(c), 1798.146(a)(1), (4), and (5).) The Agency will continue to monitor the marketplace to determine whether modifications to the regulations are necessary.
ADMT	2050	Comment argues for the adoption of a "precautionary principle" under which an algorithmic tool used to collect worker or patient data may not be adopted or implemented until demonstrably proven safe and effective.	The Agency disagrees with this comment. The CCPA directs the Agency to issue regulations governing opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a).) In addition, businesses must conduct risk assessments for processing that presents significant risk to consumers' privacy, such as processing sensitive personal information and using ADMT to make a significant decision. As part of the risk assessment, businesses must identify relevant risks to consumers' privacy and safeguards. (*See* § 7152.) Adopting commenter's recommendation is not necessary at this time.
ADMT	2055	Comment argues the ability for generative AI to mimic the appearance of human reason raises serious concerns surrounding automation bias.	The Agency agrees with this comment to the extent it supports safeguards for consumers' privacy as businesses use ADMT. However, the Agency has deleted the definition of artificial intelligence as

			unnecessary and removed corresponding references to it throughout the regulations to simplify implementation for businesses at this time. The regulations also address concerns about bias in various ways, such as via the risk assessment and the requirements for the human appeal exception. The Agency will continue to monitor the marketplace to determine whether modifications to the regulations are necessary.
ADMT	2057	Comment argues clinicians and patients should have the right to review, interpret, and explain data and clinical research underlying ADMT and AI data collection, rather than forced to trust an opaque ADMT system. High-quality patient care depends on understanding ADMT-presented information.	The Agency agrees with this comment in part, to the extent it supports transparency for consumers with respect to businesses' use of ADMT. The Agency disagrees with this comment in part, to the extent it suggests that the regulations do not provide consumers with the right to access ADMT. The regulations require businesses to provide consumers with access to ADMT. This includes information about the logic of the ADMT, and the outcome of the decisionmaking process for the consumer.
ADMT	2058-2484	Comment strongly urges the Agency to adopt its ADMT regulations as they are common sense rules that are a vital intervention for consumer protection and human rights. As unaccountable algorithms increasingly influence housing, education, employment, and basic freedoms, the rules should reflect the needs of everyday people to be protected from discrimination and data scraping, not Big Tech's appetite for profiting from personal information. Comment calls on the Agency to stand strong, defend the public's rights to algorithmic transparency and accountability, and adopt the amended regulations.	The Agency agrees with this comment to the extent that it supports further protections for consumers' privacy. Nevertheless, the Agency modified the regulations, which balance protections for consumer privacy and simplifying implementation for businesses at this time. The Agency will continue to monitor the marketplace to determine whether modifications to the regulations are necessary. The Agency looks forward to working with stakeholders on future policy development.

ARTICLES 9, 10, 11 – GENERAL COMMENTS

Section of Regulation	Comment Numbers	Summary of Comments 45-Day Comment Period	Agency Response
CS Audits / RAs	152	Comment concerned that requiring extensive documentation on cybersecurity audits and risk assessments could lead to confidentiality risks, competitive disadvantages, and increased litigation exposure. Comment argues that the Agency must implement stronger safeguards to prevent disclosure of sensitive information, including trade secrets.	The Agency disagrees with this comment. The comment's interpretation of the cybersecurity audit regulations appears to be inconsistent with the regulations' language, which requires a business to submit a certification of completion to the Agency, not its cybersecurity audit report. (*See* § 7124.) The Agency revised risk-assessment submission requirements to simplify implementation for businesses at this time, and the CCPA already provides protection for trade secrets. Additionally, providing disclosures to the Agency does not equate to it being exposed; whether information in the Agency's records is subject to public disclosure depends on the specific information and whether an exception to the PRA applies.
CS Audits / RAs	2027	The rules require businesses to perform extensive risk assessments and internal audits on systems that have little to do with the actual privacy risk voters were concerned about. It includes scrutinizing systems used for basic functions, like analyzing data and excel spreadsheets, or tracking employee performance that have been used for decades without incident. The rules would force companies to disclose internal details about how these systems operate, potentially revealing trade secrets and sensitive operational methods. Such disclosures could not only undermine competitive advantage, but also expose vulnerabilities that bad actors might exploit.	The Agency disagrees with this comment. Regarding cybersecurity audits, the CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security, to complete an annual cybersecurity audit, with the regulations establishing a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The thresholds in § 7120(b) articulate when a business's processing of consumers' personal information presents significant risk to consumers' security and focus on personal information. The comment's interpretation of the proposed regulations appears to be inconsistent with the regulations' language, which require a business to

			submit a certification of completion to the Agency, not its cybersecurity audit report. (*See* proposed § 7124.) Regarding risk assessments, the CCPA directs the Agency to require businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment and requires that risk assessments be submitted to the Agency on a regular basis. (Civ. Code § 1798.185(a)(14)(B).) Additionally, the CCPA already provides protection for trade secrets for risk assessments.
CS Audits / RAs	527	Comment advocates for aligning cybersecurity audits and risk assessments with existing global and state privacy laws.	The Agency disagrees with this comment. Regarding cybersecurity audits, the comment does not explain which laws it advocates aligning with, and there are no generally applicable state laws that require cybersecurity audits. While the Agency strives for consistency with privacy and security laws in other jurisdictions when appropriate, it must comply with California law and use its discretion to adopt requirements appropriate to California. Moreover, the regulations implement the requirements of California law, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements.
CS Audits / RAs	805	Comment asserts that exemptions for federally regulated entities exist in several sections (7022(f), 7023(f), 7024(e), 7080(g)) but are inconsistently applied. The Risk Assessment Regulation (§ 7150(b)(2)) and Cybersecurity Regulations lack similar protections for GLBA-covered data, creating discrepancies.	The Agency disagrees with this comment. The CCPA's exemptions, including those for GLBA, FCRA, and HIPAA-governed data, are already explicitly stated in the statute and apply by default. There is no requirement to reiterate these exemptions in the regulations, as doing so could create unnecessary complexity or confusion. The Agency has similarly removed references to the exemptions in the definition

			of "significant decision" to avoid similar confusion about when the exemptions apply.
CS Audits / RAs	1223, 1533	Comment contends that the Cybersecurity Audit and Risk Assessment Proposed Regulations are redundant and burdensome because federal and state regulators already impose comprehensive, risk-based cybersecurity regimes. Financial institutions comply with stringent federal standards such as the GLBA Safeguards Rule, Interagency Guidelines, and the FFIEC IT Examination Handbooks, as well as enhanced state requirements like New York's Cybersecurity Regulations. Comment argues that credit unions are already subject to oversight by the National Credit Union Administration (NCUA) and compliance with Gramm-Leach-Bliley Act (GLBA) safeguards. Imposing additional, inconsistent CCPA standards, such as requiring "zero trust architecture" or mandatory "network segmentation," would not materially improve security but would increase compliance complexity and cost. Comment requests exemption from cybersecurity audits and risk assessments under the proposed rules, citing functional equivalence with existing federal standards (Articles 9 and 10). Comment suggests the Agency consider stating in the Proposed Regulation that compliance with the existing safeguards and standards described above will be deemed as "reasonable security procedures and practices appropriate to the nature of the information to protect the personal information," and in compliance with the cybersecurity requirements in the Proposed Regulations. This may include relying on the certification, attestation, etc., requirements in existing	The Agency disagrees with this comment. Exempting financial institutions would be inconsistent with the CCPA. The CCPA includes data-level exemptions, including for (1) information subject to GLBA and implementing regulations or the California Financial Information Privacy Act, (2) information governed by HIPAA, and (3) the processing of personal information by certain entities, as long as the activity is regulated by the FCRA, and the processing is as authorized by the FCRA. (*See* Civ. Code §§ 1798.145(c)(1), (d), (e), 1798.146(a)(1), (4), (5).) However, the CCPA applies to "businesses," is intended to supplement federal and state law, and does not exempt financial institutions. (*See* Civ. Code §§ 1798.140(d), 1798.196.) Additionally, the CCPA makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196.) The CCPA requires businesses whose processing of consumers' personal information presents significant risk to consumers' security to perform an annual cybersecurity audit and requires the regulations to establish a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The CCPA also directs the Agency to require businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment, and requires that risk assessments be submitted to the Agency on a regular basis. (Civ. Code § 1798.185(a)(14)(B).) The Agency cannot amend the CCPA or adopt regulations

		safeguards and standards, instead of instituting a duplicative and/or inconsistent process.	inconsistent with the CCPA. Although the Agency strives for alignment with other privacy and security laws and existing standards when appropriate, it must comply with California law and use its discretion to adopt requirements appropriate to California. To the extent the comment suggests that the Agency deem compliance with other laws or the use of the FFIEC IT Examination Handbook as "reasonable security," that would not be consistent with the CCPA's direction to the Agency regarding cybersecurity audits. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA**.** The Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example. To the extent the comment suggests that the Agency should accept a business's use of a cybersecurity audit framework in lieu of meeting the cybersecurity audit requirements in Article 9, the Agency disagrees with that suggestion, because a business's use of another framework does not ensure that the business conducted a thorough and independent cybersecurity audit focused on securing consumers' personal information. The regulations implement the requirements of California law, are consistent with other cybersecurity frameworks, and provide businesses with flexibility in how they meet requirements. The risk assessment regulations explicitly allow a business to use a risk assessment that it has prepared for another purpose, to comply with § 7152. (*See* § 7156(b).) Therefore, to the extent a business is already complying with the risk assessment

DRAFT

			requirements in other laws, it can leverage those compliance processes to comply with the regulations. Finally, with respect to zero trust architecture, the Agency deleted the term "zero trust architecture" to simplify implementation at this time.
CS Audits / RAs	1019	Comment asserts that the proposed rules require businesses to submit risk assessments and cybersecurity audits to CPPA without any privilege protections. Many businesses conduct these assessments with legal counsel, and without protections, companies face a Hobson's choice. In addition, other state privacy laws protect privilege for such disclosures, while the proposed rules do not. Comment recommends adding into the proposed regulations protections for cybersecurity audits and risk assessments produced to the CPPA so that (a) there is no waiver of the attorney client privilege or work product doctrine and (b) the cybersecurity audits and risk assessments are exempt from open records laws disclosures.	The Agency disagrees with this comment. The risk assessment regulations do not require submission of privileged information. The cybersecurity audit regulations require a business to annually submit a certification of completion to the Agency, not its cybersecurity audit report. (*See* proposed § 7124.) Additionally, whether information in the Agency's records is subject to public disclosure depends on the specific information within the document and whether an exception to the Public Records Act applies.
CS Audits / RAs	1020	Comment states that the proposed rules (§§ 7121, 7155(c)) give businesses 24 months to complete cybersecurity audits and document risk assessments for pre-existing activities. However, new processing activities beginning right after the effective date must immediately comply, even if planned for months or years. Comment recommends providing a 6-month grace period for businesses launching new processing activities planned before the regulations take effect.	The Agency disagrees with this comment. However, the Agency revised § 7121 to phase in implementation by annual gross revenue over a three-year period, clarify the audit coverage period, provide additional time after the audit period to complete the cybersecurity audit report, and clarify the specific date by which a business must complete its cybersecurity audit report. With respect to § 7155(c), the regulation ensures that businesses identify and manage risks before initiating a processing activity that presents significant risk to consumers' privacy. Comment's recommendation would be less effective than the regulation at protecting consumers' privacy, because it would not require a

			business to conduct a risk assessment for that processing until after it has been engaging in the processing for six months. In addition, businesses that are subject to existing risk assessment requirements, such as those under the Colorado Privacy Act and GDPR, can leverage their existing compliance processes to comply with the CCPA's risk assessment requirements, as explicitly provided in § 7156(b). This provides businesses with sufficient time and flexibility to come into compliance.
CS Audits / RAs	1095	Comment believes that requiring individual executives to certify cybersecurity audits could deter professionals from taking security roles and may compromise independence. Instead, independent third-party certifications should be accepted. §§ 7124(c) and 7157(b) should be replaced with a requirement for third party auditors to work with internal audit and cybersecurity teams to conduct the cybersecurity audit for their objective expertise and ultimate collective sign-off. Conversely, the Agency should consider whether certification under a recognized security and privacy standard could satisfy the audit requirement. For example, an organization that certifies under the rigors of SOC2 Type2 (5 Trust), ISO 27001 and 27701, NIST Cybersecurity and Privacy Frameworks, FedRamp, FISMA, GDPR, or other widely accepted certifications requiring third party audits should satisfy the annual cybersecurity audit and privacy impact assessment aims of these new rules.	The Agency disagrees with this comment. The comment has provided no information to support that requiring individual executives to certify cybersecurity audits would deter professionals from taking security roles, nor has the comment explained how or why requiring executive certification would compromise the independence of an audit. § 7122 includes several provisions that establish processes to ensure the independence of cybersecurity audits, consistent with the CCPA's direction to the Agency. (*See* Civ. Code § 1798.185(a)(14)(A).) Regarding the comment's suggestion to require the use of third-party auditors, the regulations are meant to apply to many factual situations and across industries, and to be robust yet flexible to account for differences among businesses and their information systems. Comment's suggestion would impose more prescriptive obligations upon businesses. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. With respect to cybersecurity audits, the Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through

			supplementation; the Agency has also included an example. To the extent the comment suggests that the Agency should accept a business's certification related to a its use of a cybersecurity audit framework or standard in lieu of meeting the cybersecurity audit requirements in Article 9, the Agency disagrees with that suggestion, because that would not ensure that the business conducted a thorough and independent cybersecurity audit focused on securing consumers' personal information.
CS Audits / RAs	1296	Comment supports the Agency's proposed cybersecurity audit rules and advocate for external, third-party audits to ensure accountability. Comment calls for additional reporting requirements to improve transparency in AI applications and emphasize the need for adequate funding for the CPPA to effectively enforce regulations. Specifically, comment strongly suggests that external, third-party audits be emphasized in § 7122(a)(1) to provide an impartial assessment of a business's cybersecurity measures and ensure accountability. If internal audits are permitted, comment supports regulations requiring results to be subject to heightened scrutiny and third-party validation to ensure they meet the same rigorous standards as external evaluations. In addition, disclosure requirements in § 7152(a)(2)(b)(iii) should also include an explanation of the specific methods employed for removing personal information, as well as any known error rates or limitations of those methods. Additionally, § 7152(a)(3) should be amended to require businesses to disclose datasets purchased or used for model training and whether consent was obtained for	The Agency agrees in part with this comment and notes its support for the proposed cybersecurity audit rules and for adequately funding the Agency's enforcement efforts. The Agency disagrees with this comment regarding emphasizing external auditors, requiring third-party validation, and requirements relating to artificial intelligence. The proposed regulations specifically permit the use of internal auditors and are meant to apply to many factual situations and across industries, and to be robust yet flexible to account for differences among businesses. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. § 7122 establishes processes to ensure the independence of the business's annual cybersecurity audits, consistent with the CCPA's direction to the Agency. (*See* Civ. Code § 1798.185(a)(14)(A).)

		personal data included in those datasets, particularly for ADMT and generative AI.	
CS Audits / RAs	1379	The regulations should recognize a meaningful safe harbor for risk assessments and cybersecurity audits. The limited risk assessment safe harbor requires businesses to supplement existing assessments, which, in practice, renders the safe harbor an empty provision that departs from U.S. privacy statutes (e.g., Colorado, Montana, Tennessee, Texas).	The Agency disagrees with this comment. The Agency has determined that providing a safe harbor for businesses, even if the risk-assessment or cybersecurity work they have done for another purpose does not meet the requirements of the regulations, does not further the intent and purpose of CCPA, and would be inconsistent with the CCPA's direction to the Agency. With respect to risk assessments, § 7156(b) provides a clear standard for businesses about how they can use existing compliance processes to conduct a risk assessment under the CCPA. This enables interoperability while ensuring that businesses conduct risk assessments that meet the requirements of § 7152. With respect to cybersecurity audits, the Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation; the Agency has also included an example. To the extent the comment suggests that the Agency should accept a business's use of a cybersecurity audit framework in lieu of meeting the cybersecurity audit requirements in Article 9, the Agency disagrees with that suggestion, because a business's use of another framework does not ensure that the business conducted a thorough and independent cybersecurity audit focused on securing consumers' personal information.
CS Audits / RAs	1395	The CPPA's overbroad cybersecurity audits and privacy risk assessments compel speech and do not satisfy the First Amendment test of strict scrutiny. Cybersecurity	The Agency disagrees with this comment. The Agency does not believe the requirements raise concerns under the First Amendment. However, regarding the

		audits and privacy risk assessments reflect more than mere facts about a business's operations. They reflect opinions and judgments about how the business protects consumer personal information, what safeguards are appropriate, and a description of how the business has weighed risks with consumer benefits. For example, cybersecurity audits must "document and explain why [a] component is not necessary" to the business's cybersecurity efforts. The regulations' approach to privacy risk assessments likewise reflects embedded opinions about the privacy risks and benefits of processing activities, including through the identification of "negative impacts" to consumers associated with the processing, such as intangible considerations like reputational or psychological harms. Even assuming that these requirements further a compelling government interest, their sheer breadth makes plain that they are not narrowly tailored.	cybersecurity audit regulations, the Agency revised § 7123(c), previously § 7123(b)(2), to delete 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, to simplify implementation at this time. In addition, the Agency revised the risk assessment regulations to no longer require the documentation of the risks and benefits of the processing, to simplify implementation for businesses at this time. (§§ 7152(a)(4), (5).) Separately, the regulations have also removed the profiling for behavioral advertising threshold to simplify implementation for businesses at this time.
CS Audits / RAs	1777	Comment encourages the Agency to continue expanding its engagement with innovative cybersecurity and AI-driven companies. A risk-based approach, which aligns with evolving cybersecurity best practices, ensures that businesses can adapt to new threats while maintaining compliance. This approach mirrors the National Institute of Standards and Technology's (NIST) efforts to establish secure practices for AI model development, privacy, and security. Comment commends that the Agency's introduction of Article 9 (Cybersecurity Audits) and Article 10 (Risk Assessments) aligns with these principles, ensuring a structured and proactive approach to security and privacy governance.	The Agency agrees with this comment and notes commenter's support.

CS Audits / RAs	1806	Comment seeks validation of consumers' responsible behavior. Enabling consumers by reviewing cybersecurity audits and risk assessments they conduct using AI, could be a great help to all stakeholders.	It is unclear what the comment is suggesting. Nevertheless, the Agency agrees that the cybersecurity audit and risk assessment requirements in the regulations encourages responsible behavior.
CS Audits / RAs	1905	Comment argues that while § 7123 provides a comprehensive list of factors for audits, it lacks the clarity in the requirements to collect and disclose quantitative key performance metrics to the Agency. Comment suggests that § 7152 should include a requirement that cybersecurity audits collect numeric key performance indicator data wherever possible, and at the very least for the following metrics: Percent and number of organizational devices missing two or more critical software updates; Percent and number of organizational devices protected by full disk encryption; Percent and number of staff who have completed annual security training; Number of software systems for which single user accounts are being shared by multiple people. Additionally, § 7157 should require that these key metrics be included in all risk assessment submissions to the Agency.	The Agency disagrees with this comment. The CCPA directs the Agency to define the scope of the cybersecurity audit and establish a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The regulations are consistent with this direction and provide clarity about how businesses must perform a thorough and independent cybersecurity audit. In drafting the regulations, the Agency considered how to ensure that a cybersecurity audit thoroughly and independently assesses how a business protects consumers' personal information, while providing flexibility for businesses and their auditors. The regulations require a business to submit a certification of completion to the Agency, not its cybersecurity audit report. (*See* proposed § 7124.) The comment's suggestion to require the collection and reporting of specific information is not more effective or more appropriate than the Agency's proposed regulations. With respect to risk assessments, §§ 7152 and 7157 address risk assessment requirements for processing that presents significant risk to consumers' privacy. Comment's recommendations are not necessary for risk assessments at this time. The metrics requested for inclusion in § 7157 do not appear tailored to the processing activities that require a risk assessment in § 7150(b). In addition, the Agency has considered more detailed submission reporting requirements, but has simplified the submission

			requirements, including relevant metrics, to simplify implementation for businesses at this time.
CS Audits / ADMT	138, 140, 144, 148, 176, 1531	Comment warns that failing to exempt banks or revise the regulations could lead to unintended consequences, such as weakening consumer privacy protections, legal challenges, and disruptions to financial services. Comment argues that the proposed ADMT regulations limit the way financial institutions may review personal information for fraud and financial crimes, to a significant detriment to consumers, and may create safety and soundness risk. The rules could undermine fraud detection and credit risk management, if bad actors must be given information about or may opt out of the use of their data for training automated fraud detection. Comment warns that the proposed regulations interfere with federal exemptions under the CCPA for data regulated by federal laws like GLBA and HIPAA. It argues that requiring enterprise-wide cybersecurity compliance could create indirect regulatory burdens on federally regulated institutions, which contradicts the intent of the CCPA's exemptions. The proposed cybersecurity audit requirements conflict with the banking industry's more rigorous and flexible auditing practices, by introducing prescriptive cybersecurity audit requirements that seemingly require a single annual information security audit. Comment argues that financial institutions must conduct independent internal audits under board-level oversight. Regulators regularly examine banks' cybersecurity and ADMT compliance, conducting on-site reviews and enforcing corrective actions when necessary. These audits apply across GLBA-covered and non-GLBA data. Comment suggests revising §§ 7124(a) and 7157(b)(4) as follows:	The Agency disagrees with this comment. Exempting financial institutions would be inconsistent with the CCPA. Similarly, exempting a business because it is subject to examination or supervision by another regulator would be inconsistent with the purpose and intent of the CCPA. The CCPA includes data-level exemptions, including for (1) information subject to GLBA and implementing regulations or the California Financial Information Privacy Act, (2) information governed by HIPAA, and (3) the processing of personal information by certain entities, as long as the activity is regulated by the FCRA, and the processing is as authorized by the FCRA. (*See* Civ. Code §§ 1798.145(c)(1), (d), (e), 1798.146(a)(1), (4), (5).) However, the CCPA applies to "businesses," is intended to supplement federal and state law, and does not exempt financial institutions. (*See* Civ. Code §§ 1798.140(d), 1798.196.) Additionally, the CCPA makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196.) The CCPA requires businesses whose processing of consumers' personal information presents significant risk to consumers' security to perform an annual cybersecurity audit and requires the regulations to establish a process to ensure that audits are thorough and independent. (Civ. Code § 1798.185(a)(14)(A).) The CCPA also directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) Not requiring a thorough

		"Each business that is required to complete a cybersecurity audit pursuant to this Article must submit to the Agency every calendar year a written certification that the business completed the cybersecurity audit as set forth in this Article unless the business is subject to examination or supervision by a federal prudential regulator with respect to cybersecurity," and "A business is not required to submit a risk assessment to the Agency if the business does not initiate the processing activity subject to the risk assessment or if a risk assessment is undertaken in a manner that is subject to examination or supervision by a federal prudential regulator."	annual cybersecurity audit would be inconsistent with the law. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Further, the regulations are consistent with, and further the intent and purposes of, the CCPA. They balance providing privacy protections for consumers with flexibility for businesses in meeting their compliance obligations. Moreover, the Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The Agency has revised the regulations to simplify implementation for businesses at this time. For example, the Agency revised § 7123(f) to clarify that a business may utilize cybersecurity assessment work it has already done, provided that it meets all of the California requirements, either on its own or through supplementation. The Agency has also included an example of this.
CS Audits / ADMT	1163	Comment urges the Agency to ensure that its new regulations governing ADMT and cybersecurity audits preserve for Californians the ability to protect their homes and personal safety.	It is unclear what this comment is suggesting, as it does not provide sufficient information for the Agency to substantively respond. The Agency notes commenter's suggestion and looks forward to working with stakeholders on future policy development.
7150, 7200	182, 746	Comment suggests that §§ 7150(b)(3)-(4), 7200(a)(2)-(3) should be deleted in their entirety, or narrowed to remove reference to behavioral advertising. Inclusion of advertising is too broad and burdensome, deviates from other state laws, and deters businesses from providing benefits to consumers.	The Agency disagrees with this comment. Nevertheless, the Agency revised the regulations to ensure that businesses conduct a risk assessment for certain automated processing and training uses of personal information that present significant risk to consumers' privacy. The Agency also revised the risk assessment and ADMT regulations to remove the profiling for behavioral advertising threshold and the other extensive profiling and training ADMT thresholds from Article 11, to further simplify implementation for businesses at this time.

7150, 7200	1096	Comment suggests that AI governance should focus on high-risk applications, similar to frameworks like the EU AI Act and NIST AI RMF, instead of broad, blanket regulations. The proposed rules, such as § 7200(a)(1)-(3) and § 7150(b)(3)-(4), do not distinguish between AI developers and deployers, making compliance difficult. Accordingly, the Agency should hone its Proposed Rules, which are overly broad as written in a number of areas. The rules for ADMT in Article 11 would apply to any "business that uses [ADMT] in any of the following ways . . .: (1) For a significant decision concerning a consumer . . . (2) For extensive profiling of a consumer . . .[or] (3) For [certain] training uses of [ADMT]." Likewise, the rules for Risk Assessments in Article 10 would in relevant part apply to any business (1) "[u]sing [ADMT] for a significant decision concerning a consumer or for extensive profiling" or (2)[p]rocessing the personal information of consumers to train [ADMT] or [AI] that is capable of being used for [certain uses].	The Agency disagrees with this comment. The regulations provide clarity about what is in scope and are not overly broad. The Agency also has revised the regulations, including focusing § 7200 on significant decisions and revising the thresholds in § 7150(b), to further simplify implementation for businesses at this time. Further, with respect to developers and deployers, the regulations clearly and specifically address the responsibilities of businesses in Articles 10 and 11, and the responsibilities of service providers and contractors in § 7050.
7150, 7200	1858	Comment suggests clarifying in §§ 7150(b)(4)(B) and 7200(a)(3)(B) what it means for an ADMT or AI system to be used for "establish[ing] individual identity."	The Agency disagrees with this comment. The regulation is clear about what processing is in scope. In addition, the regulation has been revised to provide further clarity about what training uses of personal information are in scope for risk assessment, and to remove the training uses of ADMT from Article 11's requirements.
7150, 7221	1203, 1221, 1232, 1310, 1916, 1951	Comment believes that the term "significant decision" lacks clarity, overly broad and include non-material impacts, and subjective. It also diverges from other state laws. This makes it difficult for businesses to determine compliance obligations. The regulations provide only a few vague examples, leaving many industries uncertain about whether their practices are	The Agency disagrees with this comment. The definition of significant decision is reasonably clear about what is a significant decision. Additionally, the Agency has revised the definition to provide further clarity about the types of decisions that are subject to the regulations, and deleted certain terms, such as "access" and "essential goods or services," to simplify

		covered. The proposed definition also includes low-risk decisions, potentially deterring businesses from offering AI-enhanced services in California. Comment therefore suggests striking from the definition of "significant decision" — and associated portions of the regulations — references to (a) "access," and (b) "allocation or assignment of work." Comment also suggests revising the definition to align with existing standards or focusing on denying essential services.	implementation for businesses at this time. Similarly, with respect to allocation or assignment of work, the Agency has revised this to only apply to employees to simplify implementation for businesses at this time. Comment's suggestion to only focus on denial of essential services is also less effective at protecting consumer privacy than the regulation, which focuses on both the provision or denial of certain enumerated goods and services.
7150, 7221	1371, 1577	Comment suggests limiting heightened regulatory obligations to the processing of personal information that "presents significant risk to consumers' privacy or security", as required by the CCPA. Comment argues that prescriptive classifications of technologies or of processing activities as "significant risk" should be avoided, unless required by the statute. ADMT opt-outs should align with U.S. state privacy statutes and global frameworks that limit opt-outs to ADMT used in furtherance of decisions with legal or similarly significant effects – specifically, significant decisions made without human involvement and that present a significant risk to consumer privacy. It should not include ADMT training or "access to" certain opportunities. This would help address the overly broad scope of significant decisions as compared to other state privacy frameworks and the CPPA's overreach into areas not germane to its role as a privacy regulator. To the extent regulations nevertheless classify a certain technology or processing activity as presenting significant risk (especially in the absence of a statutory mandate), businesses should be able to treat such classifications as rebuttable presumptions.	The Agency disagrees with the comment. The regulations are within the Agency's authority and further the intent and purposes of the CCPA. Each of the thresholds in § 7150(b) presents a significant risk to consumers' privacy and requires a risk assessment. In addition, businesses must provide consumers with the ability to opt-out and access their use of ADMT. Further, comment's proposed rebuttable recommendation is less effective than the regulation at protecting consumer privacy. It is less clear than the regulation because it does not clearly indicate how a business would rebut the classification of a processing activity in § 7150(b) as a significant risk. The regulations also provide sufficient guidance to businesses regarding the thresholds and how to conduct a risk assessment and are both practicable and scalable. Nevertheless, the Agency modified the definition of ADMT to focus on a higher-risk use of ADMT at this time, which is a use without any human involvement. The Agency also revised the definition of significant decision and § 7200 to focus on the use of ADMT for significant decisions. These modifications balance protections for consumer privacy and simplifies implementation for businesses at this time. The modified regulations are consistent with

			approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope.
7155(a)(2), 7221(c)(1)	1461	In § 7155(a)(2), delete the language "before initiating any processing activity identified in § 7150, subsection (b)." In § 7221(c)(1), revise to state that a business may allow the consumer to submit request through an interactive form provided on their website or in the privacy policy.	The Agency disagrees with this comment. The commenter's suggested language is less clear than the regulation because it does not specify when a risk assessment must be conducted. It also does not benefit businesses or consumers. By contrast, the regulation ensures that businesses identify and manage risks before initiating a processing activity. With respect to § 7221(c)(1), commenter's recommendation is less effective than the regulation at protecting consumers' privacy because it fails to ensure that consumers have an easy way to submit opt-out requests online with a clearly labeled link. By contrast, the regulation makes clear that businesses must provide an opt-out link in the Pre-use Notice with a link title that states what the consumer is opting out of. This ensures consumers can meaningfully exercise their opt-out right at a time when they are given information about how an ADMT will be used to make a significant decision about them.
7157, 7221	187	Comment suggests the addition of § 7221(b): "A business is not required to provide consumers with the ability to opt-out of a business's use of automated decisionmaking technology in the following circumstances: (1) The business's use of that automated decisionmaking technology is for security, fraud prevention, or safety purposes, including but not limited to the purposes listed below ("security, fraud prevention, and safety exception"): (A) To prevent, detect, and investigate security incidents that	The Agency disagrees with this comment and has removed the security/fraud-prevention/safety exception as unnecessary because the Agency modified the definition of ADMT to focus on a higher-risk use of ADMT at this time, which is a use without any human involvement. The Agency also revised the definition of significant decision and § 7200 to focus on the use of ADMT for significant decisions. This balances protections for consumer privacy and simplifies implementation for businesses at this time.

		compromise the availability, authenticity, integrity, or confidentiality of stored or transmitted personal information or the availability, integrity, or confidentiality of information systems, or otherwise help ensure security and integrity of personal information or information systems; (B) To resist malicious, deceptive, fraudulent, or illegal actions and to prosecute those responsible for those actions; (C) To ensure the physical safety of natural persons; (D) To otherwise ensure security and integrity; or (E) To comply with laws, including any regulation or guidance implementing such laws." Comment notes that "security and integrity" is already defined in the CCPA and that conforming changes should be made elsewhere, including striking references to "direct at the business" in §§ 7027(m)(3) and 7157(b)(2)(D). In addition, comparable changes should be made to similar language in the regulations, such as § 7157(b)(2)(D).	Separately, the Agency revised the regulations to expand security/fraud-prevention/safety exceptions elsewhere within the regulations to cover malicious activities directed at consumers. (*See* §§ 7220(d)(2)(B), 7222(c)(2)(B), 7027(m)(3).) With respect to § 7157(b)(2)(D), this regulation has been deleted because abridged risk assessments are no longer part of the risk assessment submission requirements.
7157, 7222	1687	Comment states that exceptions for security, fraud detection, and safety should be construed narrowly in §§ 7157(b)(2)(D) and 7222(b)(4)(D). Businesses have often used fraud prevention and detection as a cover to collect broad swaths of data, which exposes consumers to privacy harms and unnecessary risks of data breaches. There are also examples of fraud detection systems in the public benefits context falsely flagging individuals and these systems producing discriminatory outputs and having biases. Businesses should not be able to use fraud as a blanket excuse to avoid any disclosure about how the ADMT worked with regard to the consumer if the disclosure would not compromise the functioning of the system. The regulations should include a provision similar to	The Agency agrees in part with this comment, to the extent it states that security, fraud prevention, and safety are not blanket excuses to avoid disclosures and that exceptions should not be subject to abuse. With respect to § 7222, the Agency disagrees with the comment to the extent it does not think the regulations adequately address their concerns. Businesses must still provide the information required in § 7222(b) to a consumer. They are not required to provide certain security, fraud prevention, and safety information, but they must provide meaningful information to the consumer in response to an access ADMT request. A business cannot provide a generic explanation under the access ADMT requirements, so additional explanation of why the business cannot provide the

		§ 7220(c)(1) where businesses must provide a Pre-use Notice with "plain language explanation of specific purpose" and cannot use generic terms like "to improve our services." Businesses should also be required to provide a sufficiently detailed reason as to why disclosure will compromise the functioning of the system rather than just a generic explanation.	security, fraud prevention, and safety information is not necessary. Further, the regulations in § 7222(b)(1) already require businesses to identify a purpose with specificity and prohibit describing the purpose in generic terms. The access ADMT requirements balance providing meaningful information to the consumer in response to an access ADMT request, with ensuring that businesses do not disclose certain security, fraud prevention, and safety information. The Agency does not believe removing or narrowing the exemption regarding security, fraud prevention, and safety in §§ 7220 and 7222 is necessary at this time. In addition, § 7157 has been revised and the safety, fraud prevention, and safety exception has been removed as unnecessary.
RAs / ADMT	80, 110, 111, 113, 114, 116, 117, 488, 489, 490, 492, 515, 516, 561, 562, 1085, 1509, 2032	Data-driven technologies are transforming workplaces across various industries, including trucking, healthcare, retail, hospitality, and the public sector. While these technologies can offer benefits, the lack of clear regulations raises concerns about transparency and worker protections. Studies highlight risks such as excessive workplace surveillance, algorithmic bias in hiring, and the potential for increased workload and injuries. Without proper safeguards, these advancements may disproportionately harm vulnerable worker groups, including people of color, women, and immigrants. Comment highlights the need for stronger protections as AI-driven technologies are already affecting workers. The regulations do not adequately address the risks posed by ADMT in terms of economic losses, discrimination, and psychological harm. Comment calls for risk assessments, transparency, opt-out rights, and stronger oversight. To safeguard workers, risk assessments should be strengthened,	The Agency agrees with the comment in part. Workplaces are changing and clear regulations are necessary to safeguard consumer privacy in these settings. The Agency disagrees with the comment, to the extent it suggests that the regulations do not adequately address risks. The regulations provide clear requirements and guidance to businesses for conducting risk assessments and providing ADMT opt-out and access rights. They also provide safeguards against privacy harms in the workplace, such as lack of transparency over the processing of personal information and discrimination based upon protected characteristics. With respect to economic harm, discrimination, and psychological harm, the regulations provide explicit guidance regarding these negative impacts in the risk assessment regulations. This provides guidance to businesses with identifying these harms to workers when conducting their risk assessments. The risk assessment requirements

		including the role of workers and unions and the power of the CPPA to act on risk assessments; the definition of ADMT should be expanded; notice and access rights for ADMT should be strengthened; and workers and consumers should have the right to opt out of consequential ADMT decisions. Comment suggests that employers should be required to provide strong notice and risk assessments before deploying AI technologies in hiring and workplace management. This would allow workers to understand and respond to potential risks before experiencing harm. Comment also states that the Agency should add a clear rule and mechanism for the Agency and workers and consumers to challenge a company's risk assessment or the efficacy of safeguards implemented by a company. By allowing companies to set their own standards for risk assessment and risk mitigation without Agency authority to review for compliance, businesses can simply assert that the benefits of ADMT outweigh the risk to consumers and workers. Comment argues that the proposed regulations lack a clear process enabling the Agency to dispute a company's self-certified determination that processing benefits outweigh risks, as required under Civil Code § 1798.185(a)(15)(B). Comment proposes adding language to allow the Agency to require more evidence, hold a hearing, and restrict or prohibit unlawful processing. Comment suggests strengthening notice and access rights for workers and restoring opt-out rights.	provide protections for consumers' privacy while ensuring that they are adaptable to a variety of use cases, industries, and contexts. Additionally, § 7151 provides businesses with guidance that they may include external parties in the risk assessment, which may include these stakeholders. As with other violations of the CCPA, the Agency has enforcement authority if a business is not complying with the law. The Agency has revised the definition of ADMT to focus on human involvement, which balances providing protections to consumers with flexibility for businesses to come into compliance with these regulations. Moreover, §§ 7220, 7221, and 7221 already provides that consumers, including workers, must receive a Pre-use Notice and have the rights to opt-out of and access ADMT for significant decisions.
RAs / ADMT	143, 1228, 1021, 1227	Comment asserts that federally regulated financial institutions, including banks, credit unions, broker-dealers, investment advisers and their representatives, that are subject to a federal financial regulatory	The Agency disagrees with this comment. The CCPA includes data-level exemptions, including for information subject to the Gramm-Leach-Bliley Act and implementing regulations or the California Financial

		regime should be expressly exempt from the regulations. Financial institutions are already subject to robust cybersecurity, data protection, risk management, and other protocols as well as the vigorous examination and enforcement authority of federal financial regulators. Federal regulators closely monitor banks' and credit unions' use of AI and ADMTs. Financial institutions are already subject to model risk management guidance, which requires risk assessments, validation, governance oversight, and transparency measures. Laws like the Equal Credit Opportunity Act (ECOA) and FCRA provide safeguards against biased or unfair automated decisions, whether decisions are made by humans or AI. An exemption aligns with the spirit of the CCPA. Additional regulations are unnecessary and would only duplicate existing federal compliance requirements.	Information Privacy Act, and for the processing of personal information by certain entities, if the activity is regulated by the FCRA, and the processing is as authorized by the FCRA. (*See* Civ. Code §§ 1798.145(d), (e), 1798.196.) But the CCPA applies to "businesses" and is intended to supplement federal and state law; it does not exempt financial institutions. (*See* Civ. Code §§ 1798.140(d), The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; the CCPA's exemptions apply to the regulations. Further, the CCPA directs the Agency to issue regulations that require cybersecurity audits, risk assessments, and access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(14)-(15).) To the extent a business is using personal information in a manner set forth in Articles 9-11, it must comply with those requirements. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. Finally, the regulations have also been revised to further simplify implementation for businesses at this time.
RAs / ADMT	254, 275, 484, 536, 652, 1018, 1052, 1090, 1170, 1312, 1416, 1548, 1857, 1878, 1952	Comment contends that risk assessments and the opt-out of ADMT should focus on high-risk AI applications rather than imposing a blanket requirement. Comment criticizes the draft regulations for misunderstanding technology and imposing obligations on AI training that do not provide consumer benefits. Training a model does not involve decisions directly impacting specific consumers, and the "capable of being used" standard is overly broad and does not effectively target high-risk AI processing. Extending the requirements to such models is impractical and would impose unnecessary burdens without improving consumer privacy. Comment criticizes the assumption that training ADMT	The Agency disagrees with this comment. The CCPA requires risk assessments for processing activities that present significant risk to consumers' privacy, regardless of whether they render a significant decision about a consumer. This includes training uses of consumers' personal information. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. With respect to other jurisdictions, the training threshold is consistent with the GDPR's framework for DPIAs. Further, AB 2013 is not a risk assessment law, it is a law that requires certain disclosures to the public. The risk assessment regulations are not about public disclosures of training

		is inherently problematic and warns that restricting AI training could reduce accuracy and fairness. The regulations already provide sufficient privacy protections, such as allowing consumers to opt out of data sharing. Furthermore, no other state privacy law or AI regulation treats model training as a high-risk activity, and California's recent AB 2013 already addresses disclosure requirements related to data. Requiring disclosure of intended outputs, logic, and expected profits is excessive and goes beyond GDPR standards. Comment recommends removing training thresholds in Articles 10 and 11, and the corresponding training and AI definitions. Alternatively, comment recommends revising "capable of being used" standard to "used for" or tie training to use for a significant decision, or narrowed using standards such as intended, reasonably likely, or reasonably foreseeable. Otherwise, the regulations are beyond the Agency's authority.	data, but rather are focused on providing clarity about how to conduct a risk assessment for processing activities that present significant risk to consumers' privacy. Nevertheless, the Agency has revised the training threshold in risk assessments to remove references to AI and replaced it with an intent-based standard to further simplify implementation for businesses at this time. With respect to the opt-out of ADMT, the Agency has removed training uses of ADMT threshold from Article 11 to further simplify implementation for businesses at this time.
RAs / ADMT	337, 453, 483, 485, 499, 507, 1011, 1017, 1123, 1368, 1710, 1711, 1805	Comment argues that regulating advertising, including behavioral advertising and first-party advertising, contradicts Agency's statutory authority and exceed the Agency's privacy-focused mandate. The statute expressly excludes from its scope personal information arising from activities with "the business, distinctly branded internet website, application, or service with which the consumer intentionally interacts." Comment criticizes classifying first-party advertising as automated high-consequence decision-making. Comment warns that the regulations would disrupt ad-supported services that disproportionately benefit low-income Californians and small businesses. Comment contends that the behavioral advertising opt-out would force consumers into "all-or-nothing" choices,	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purpose of the CCPA. (*See* Civ. Code §§ 1798.185(a)(14)-(15).) With respect to pop-ups, the regulations provide flexibility for businesses on consolidating notices, as explained in §§ 7220(a), (e). However, the Agency has revised the regulations to remove the definition of behavioral advertising, and to remove the profiling for behavioral advertising threshold, to simplify implementation for businesses at this time.

		undermining consumer control and threatening the viability of ad-supported services. Comment argues that requiring consent pop-ups could confuse consumers, causing them to opt out of personalized ads unintentionally, which would harm businesses reliant on behavioral advertising. Consumers who opt out of advertising and AI training model may miss opportunities to purchase goods and services. Comment recommends removing "behavioral advertising" provisions entirely, as they are mismatched with the concept of "automated decisionmaking" and likely to lead to increased consumer confusion over the exercise of privacy rights and overwhelm consumers with unnecessary and confusing notices. At a minimum, the CPPA should remove "profiling for behavioral advertising" from the proposed regulations' ADMT opt out requirements, due to the tension with the text of the CCPA and the potential to undermine rather than advance consumer privacy interests. Comment argues that these restrictions will harm small businesses by limiting their ability to use personalized advertising and compete with larger firms.	
RAs / ADMT	484, 1704	Comment agrees heightened regulation for ADMT used in consequential decisions but criticizes the Proposed Regulations for applying prescriptive obligations to low-risk uses, such as first-party advertising. Comment argues this dilutes regulatory focus, adds unnecessary burdens, leads to notice fatigue, and contradicts both the CCPA and international norms. Risk assessments should be triggered only when ADMT is the sole basis for significant decisions. Comment also warns that risk assessments and opt-out mechanisms for first-party	The Agency agrees with this comment to the extent that it supports the Agency's regulations. The Agency disagrees with this comment to the extent it does not support the Agency's regulations. The CCPA requires risk assessments for processing that presents significant risk to consumers' privacy; they should not be restricted to when ADMT is the sole basis for significant decisions. Nevertheless, the Agency revised the definition of ADMT to focus on a higher-risk use of ADMT at this time, which is a use without any human involvement. The Agency also revised the uses of

		advertising will undermine ad-supported business models, leading to higher costs for consumers.	ADMT that require a business to comply with Article 11's requirements to focus on the use of ADMT for significant decisions. These changes were made to simplify implementation at this time. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA.
RAs / ADMT	501, 886, 1198, 1474, 1537, 1660, 1981	Comment argues that the proposed regulations may violate the First Amendment by restricting how businesses use and communicate consumer data, amounting to unlawful regulation of speech. The rules compel speech and regulate communicative content like targeted ads, invoking heightened scrutiny per *Sorrell v. IMS Health*. Comment asserts that requiring businesses to perform risk assessments on advertising compels commercial speech. Comment criticizes draft ADMT rules for restricting the use of first-party data for advertising, arguing this violates the First Amendment and conflicts with the CCPA's original scope. A consumer right to opt out of all first-party advertising would unreasonably hinder businesses lawful and constitutionally protected commercial speech. The rules inappropriately extend to First Amendment-protected publisher activities involving ADMT, such as content curation and investigative journalism. The Supreme Court has long held that advertising is a form of commercial speech that protects businesses in their right to free expression and consumers in their right to receive accurate information through advertising. Also, these uses do not implicate consumer privacy and are outside the CPPA's authority.	The Agency disagrees with this comment. The Agency does not believe the requirements raise concerns under the First Amendment. Separately, the regulations have also removed the profiling for behavioral advertising threshold to further simplify implementation for businesses at this time.
RAs / ADMT	549, 1511	Comment warns that overly broad trade-secret claims can obstruct transparency critical for public safety and	The Agency disagrees with this comment, to the extent it suggests that the regulations do not provide

		individual rights. Comment recommends that the Agency ensure information that is publicly available or readily ascertainable should not be shielded by the trade secret exception; information that has not been adequately protected should not be shielded by the trade secret exception; the "value" of the information must be properly determined; and the organization claiming trade-secret protection must not have acquired the information improperly. Comment urges that the regulations should clearly ensure that the laws' protection for trade secrets do not undermine the public and the Agency's ability to understand how businesses use Californians' personal information.	appropriate exemptions for trade secrets. The exemptions for trade secrets are clear and are not overly broad. Additionally, a business that improperly claims the trade secret exemption for information that is not a trade secret would violate the CCPA. As with other violations of the CCPA, the Agency has enforcement authority if a business is not complying with the law.
RAs / ADMT	889, 1358, 1359	Revise the regulations to clarify that all statutorily mandated exemptions are incorporated to avoid impermissible inconsistencies between the regulations and the statutory text. The Agency cannot cherry-pick which broad statutory exemptions it would like to apply in different scenarios. The regulations only identify an exception to the ADMT opt-out right when the business uses ADMT that is "necessary to achieve" and "used solely" for security, fraud prevention, and safety, but this exemption overlaps with existing statutorily-created exemptions (e.g., to exercise or defend legal claims, to comply with the law or legal process, to protect the rights of others, and where a natural person is at risk of death or serious physical injury). Comment suggests that the proposed regulations should clarify that CCPA exemptions extend to ADMT rules, such as those in §§ 7152(a)(3)(g), 7220(c)(5), and 7224(b).	The Agency disagrees with this comment and has removed cross references to the CCPA's data-level exemptions from the ADMT Article as unnecessary. The CCPA is reasonably clear in addressing which organizations and data are subject to the CCPA. All of the CCPA's exemptions apply to the regulations, and the Agency has not and cannot amend the CCPA or adopt regulations inconsistent with the CCPA. In addition, the Agency removed the security, fraud prevention, and safety exception because it is unnecessary.
RAs / ADMT	922, 1709	Comment argues that §§ 7150(b)(3), 7150(b)(4), and 7150(b)(3)(B)(iii) are too broad and vague when compared to other state privacy laws. Significant	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purpose of the CCPA, as

		decisions are not limited to the provision or denial of enumerated services and include "access to." The training threshold requires risk assessments for AI tools merely "capable of being used" for certain purposes, leading to unnecessary assessments. Similarly, profiling for behavioral advertising should only include profiling that presents a reasonably foreseeable risk of certain enumerated harms. Comment also suggests that the Agency should delete "extensive profiling" and training of ADMT or AI as triggers for ADMT or risk assessment obligations. These thresholds are inconsistent with the statute, which should only apply to uses of ADMT for significant decisions and will cause notice fatigue and undermine consumer engagement. To correspond with those changes, the Agency should also modify the example set forth in § 7150(c)(4). The requirements tied to technology "capable of" particular processing should be deleted.	amended by the California Privacy Rights Act, which California voters overwhelmingly supported via passage of Proposition 24 in 2020. (*See* Civ. Code § 1798.185(a)(14)-(15).) The risk assessment regulations target processing that presents significant risk to consumers' privacy and provide clarity about what is in scope. Nevertheless, to simplify implementation for businesses at this time, the Agency has revised the risk assessment thresholds to include using an intent-based standard for the training threshold, removed "access to" from the definition of "significant decision," and removed the profiling for behavioral advertising threshold. The example in § 7150(c)(4) has also been revised to reflect these changes. Similarly, the ADMT regulations in Article 11 no longer include the extensive profiling and training thresholds. With respect to notice fatigue and undermining consumer engagement, it is unclear how the regulations will lead to either issue, particularly because businesses can consolidate their Pre-use Notice.
RAs / ADMT	983	Comment suggests that the definition of "extensive profiling" in Articles 10 and 11 should be streamlined.	The Agency disagrees with this comment. However, exercising its discretion, the Agency removed the extensive profiling thresholds from the risk assessment and ADMT regulations. For risk assessments, the Agency instead addresses certain automated processing that infers information about an applicant, student, or worker, or is based upon a consumer's presence in a sensitive location. (*See* §§ 7150(b)(4)-(5).) For ADMT, the Agency instead focuses on the use of ADMT for significant decisions to simplify implementation at this time.

RAs / ADMT	1068	Comment argues that data privacy protections should extend beyond how data is collected to how it is used, ensuring individuals have control over decisions impacting their lives. Comment calls for developers to conduct risk assessments, disclose data usage, and allow consumers to opt out of algorithmic decision-making.	The Agency agrees with this comment, to the extent it supports the regulations' requirements for risk assessments, notices, and the opt-out of ADMT.
RAs / ADMT	1089, 1311, 1321, 1364, 1546, 1623	Comment states that the definition of "extensive profiling" conflicts with the CCPA's exemption for publicly available information and creates disproportionate compliance burdens. The risk assessment requirement could unintentionally restrict security tools that analyze video footage in public spaces. Comment recommends striking § 7150(b)(3)(B) in its entirety or striking only § 7150(b)(3)(B)(ii) (public profiling). Alternatively, clarify it refers to physical spaces with no reasonable expectation of privacy or covers data that is inherently sensitive or potentially harmful to consumers. Comment also states that the regulation should specify it does not apply to technology using publicly available or publicly observable information, or that it only applies where AI technology is used for a significant decision.	The Agency disagrees with this comment. The regulations do not conflict with the definition of publicly available information. Publicly available information does not include profiling consumers in publicly available places. However, exercising its discretion, the Agency has removed this threshold from the risk assessment requirements. It has been replaced with a threshold that addresses certain automated processing based upon a consumer's presence in a sensitive location, which refers to certain enumerated physical places. (*See* § 7150(b)(5).) With respect to burden, the regulations balance providing privacy protections to consumers with flexibility for businesses to come into compliance. Further, comment's recommended language is less effective at protecting consumer privacy than the regulation. The regulation provides clarity about what is in scope and ensures that businesses conduct a risk assessment prior to using certain automated processing based on a consumer's presence in a sensitive location. With respect to the ADMT requirements in Article 11, this threshold has been removed to simplify implementation for businesses at this time.
RAs / ADMT	1093	Comment suggests that the Agency consider amending §§ 7150 and 7200(a)(1) to more closely align with the Colorado AI Act's definition of "consequential	The Agency disagrees with the comment. However, the Agency revised the definition of ADMT to focus on a higher-risk use of ADMT at this time, which is a use

		decision," such as "a decision that has a material legal or similarly significant effect on the provision or denial to any consumer of, or the cost or terms of: (a) Education enrollment or an education opportunity; (b) Employment or an employment opportunity; (c) A financial or lending service; (d) Health-care services; (e) Housing; (f) Insurance; or (g) A legal service." Alternatively, if the Agency decides to retain reference to "criminal justice," it should clearly define the term to mean decisions related to risk assessment for pretrial hearing, sentencing, and parole.	without any human involvement. This balances protections for consumer privacy and simplifying implementation for businesses at this time. Separately, the Agency revised the definition of significant decision, and revised § 7200 to focus on the use of ADMT for significant decisions to simplify implementation at this time. As revised, the regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope.
RAs / ADMT	1105, 1143	Comment opposes the CPPA's proposed regulations, arguing that they pose economic and legal challenges. Comment urges reconsideration of the regulations to balance privacy protections while avoiding harm to the real estate industry and homeownership. Comment also requests potential exemptions or amendments to prevent market disruptions.	The Agency disagrees with this comment. The regulations balance providing privacy protections to consumers with flexibility for businesses to come into compliance. The regulations also harmonize with other jurisdictions, such as Colorado, while furthering the intent and purpose of the CCPA. The regulations provided clarity and guidance to businesses regarding the scope of their obligations. The regulations have also been revised to further simplify implementation for businesses at this time.
RAs / ADMT	1111, 1542, 1578	Comment expresses concern that the proposed rules might require businesses to disclose proprietary or confidential information about their automated systems, which could compromise intellectual property and competitiveness. They argue the regulations must explicitly safeguard trade secrets in line with statutory protections. While comment supports plain-language disclosures, it recommends exempting proprietary information, such as algorithm specifications, to protect competitive advantages while still providing sufficient transparency. Comment suggests clarifying	The Agency disagrees with this comment. The CCPA already provides protection for trade secrets for risk assessments. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The regulations for Pre-use Notices and the right to access ADMT have also been revised to clarify that when a business provides the required information for a Pre-use Notice and a response to an access request, it is not required to disclose trade secrets.

		that businesses are not required to disclose trade secrets and intellectual property rights in response to verifiable consumer requests and risk assessment submissions.	
RAs / ADMT	1152	Comment appreciates the Agency's efforts and its inclusion of examples in the proposed regulations, but it encourages the Agency to add more examples to help businesses better understand their obligations.	The Agency notes commenter's support. However, the Agency has determined that no further clarification is needed at this time. The regulations are reasonably clear and provide guidance, including through examples, where necessary.
RAs / ADMT	1191, 1915	Comment argues that the proposed regulations define "significant decisions" and "extensive profiling" too broadly, covering routine business practices that do not pose privacy concerns. The Statement of Reasons ("ISOR") fails to link these definitions to actual privacy risks. Further, the regulations should not be limited to ADMT-based uses, but on significant decisions specifically. What matters is that these decisions were made, not how they were made.	The Agency disagrees with this comment. The ISOR, as well as other public comments, have identified harms to consumers' privacy from the use of ADMT for significant decisions and extensive profiling. Nevertheless, the Agency has revised the regulations, including focusing § 7200 on significant decisions and revising the thresholds in § 7150(b), to further simplify implementation for businesses at this time.
RAs / ADMT	1217, 1218	Comment suggests that there may be a need for guidance or further examples to show how businesses should implement the principle of human intervention for high consequence decisions in practice. Comment suggests that it would be helpful to receive guidance from the Agency, wherever possible, on opportunities for companies to streamline various risk assessment obligations. For example, the Agency can offer demonstrative examples of equivalently strong ADMT risk assessments.	The Agency disagrees with this comment, to the extent it argues that additional regulations are necessary. The regulations are reasonably clear and have been revised to provide additional clarity and guidance to businesses.
RAs / ADMT	1235, 1241, 1262, 2028	The rules impose burdensome opt-out requirements that require companies to develop new systems to handles these opt-out requests for routine business processes, including first-party advertising. Comment	The Agency disagrees with this comment. The CCPA requires the Agency to issue regulations governing opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency has made

		believes that the broad scope of the rule will create significant compliance burdens for businesses, including those using simple automation tools like logistics optimization, which do not pose significant risks. Businesses will have to halt certain services if they can't feasibly accommodate these requirements, ultimately harming consumers rather than protecting them. Comment argues the proposed regulations would reduce the effectiveness of digital advertising and marketing, making customer outreach more expensive and limiting small businesses' ability to compete with larger companies. The regulations would limit businesses from directly advertising to their customers based on past purchases, a common and beneficial marketing practice. Comment argues that this would make it harder for consumers to access relevant services.	efforts to limit the burden of the regulations while implementing the CCPA. The regulations enable businesses to leverage existing processes for other CCPA rights and existing opt-out methods. The Agency has also revised the ADMT regulations to focus on the use of ADMT for significant decisions to simplify implementation at this time. These revisions include removing the profiling for behavioral advertising threshold. Further, the regulations include exceptions to opt-out of ADMT requirements.
RAs / ADMT	1363	The proposed requirements for "extensive profiling" of students and workers are redundant because they are already addressed through the opt-out right, access right, and risk assessment requirements for the use of ADMT to reach "significant decisions," which the regulations broadly define to include hiring, promotion and demotion, and termination decisions. Because the statute defines profiling as automated processing "to evaluate certain personal aspects concerning that natural person," requirements for significant decisions already encompass those activities that the regulations describe as "extensive profiling."	The Agency disagrees with this comment. Risk assessments are required for processing activities that present significant risk to consumers' privacy, regardless of whether they render a significant decision about a consumer. Nevertheless, the regulations have been revised to simplify implementation for businesses at this time. Those modifications include the removal of the extensive profiling threshold from the ADMT regulations and narrowing the corresponding threshold in risk assessments to certain automated processing.
RAs / ADMT	1365	The definition of extensive profiling does not take into account that the CCPA does not require a business to reidentify or relink information that in the ordinary course is not maintained in a manner that would be	The Agency disagrees with this comment. The regulations do not amend the CCPA. The regulation applied to profiling based on systematic observation of a publicly available place and did not include activities

		considered personal information. As a practical matter, the expansive scope of the public profiling concept will capture a number of everyday activities, such as identifying where delivery vehicles or IT assets are located.	that did not meet those requirements. Nevertheless, to simplify implementation for businesses at this time, the public profiling threshold has been removed from the requirements. The regulations now only address certain automated processing based on sensitive locations in risk assessments.
RAs / ADMT	1367	To the extent that the extensive profiling in public places concept is intended to address mass facial recognition, those concerns are already addressed separately through the existing requirements related to the processing of biometric data.	The Agency disagrees with this comment. The risk assessment threshold addresses certain automated processing of consumers' personal information based on their presence in sensitive locations, which may include automated processing via facial recognition. More broadly, a business may be engaged in a processing activity that meets more than one threshold in § 7150(b). The business must conduct a risk assessment for that activity, so long as one threshold is met. Separately, to simplify implementation for businesses at this time, the public profiling threshold has been removed from the requirements. The regulations now only address certain automated processing based on sensitive locations in risk assessments.
RAs / ADMT	1369	Through the "extensive profiling" concept, the CPPA is acting beyond the scope of its authority and pursuing a course of action that the Legislature has already rejected. The California Legislature previously considered, and declined to advance, employee privacy legislation that would have addressed ADMT. The proposed Workplace Technology Accountability Act ("WTAA") would have required employers that use ADMT to make or assist in an employment-related decision to complete an "Algorithmic Impact Assessment" prior to using the system, which would have involved comparing the risks and benefits of using	The Agency disagrees with this comment. Regulating extensive profiling is within the CCPA's delegation of authority to the Agency and is consistent with the intent and purposes of the statute. In addition, commenter's citation to legislation appears to misread CCPA. Voters already require risk assessments and ADMT rights for consumers, including employees and independent contractors, via the Proposition 24 ballot initiative. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. Whether the legislature passes other laws does not weaken the CCPA's existing requirements. Nevertheless, the

		the ADMT. The WTAA would also have granted employees the right to access whether their data was being used as an input in ADMT or generated as an output of ADMT, required employers to provide notice prior to using ADMT, and prohibited employers from using ADMT to make certain predictions about an employee's behavior (among other prohibitions). The WTAA, which the Legislature declined to act upon in the 2021-2022 Regular Session, has never been reintroduced and would have chilled innovation, made workplaces less safe, and penalized small businesses for even good faith mistakes.	Agency deleted the extensive profiling threshold from Article 11 and has revised § 7200 to focus on the use of ADMT for significant decisions to simplify implementation at this time. With respect to risk assessments, businesses must conduct a risk assessment when using ADMT for a significant decision and for certain automated processing that presents significant risk to consumers' privacy, as set forth in § 7150(b).
RAs / ADMT	1399	The regulations seek to regulate areas that are preempted by federal law. The Supremacy Clause of the U.S. Constitution prohibits states from regulating conduct "in a field that Congress, acting within its proper authority, has determined must be regulated by its exclusive governance." State laws are also preempted when they conflict with federal law, including when they stand "as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." Federal law protects trade secrets under the Defend Trade Secrets Act ("DTSA"), including "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes" that are kept "secret" and have "independent economic value . . . from not being generally known." While the DTSA does not "preempt or displace any other remedies provided by United States Federal [or] State . . . law for the misappropriation of a trade secret," California may not	The Agency disagrees with this comment. The regulations do not conflict with federal law. In addition, § 7222(c) of the revised regulations state that a business is not required to include trade secrets when providing the information required in § 7222(b)

		entirely abrogate the protections granted to a business's trade secrets. The regulations ignore the express trade secret exemption in the CCPA. For example, § 7222 requires a business to share commercially sensitive information with consumers, including the logic, assumptions, limitations, and key parameters of ADMT. Depending on the technology and business in question, and the level of detail expected by regulators, this information could constitute a business's trade secrets, required disclosure of which is preempted by federal law.	
RAs / ADMT	1479	Comment criticizes the proposed regulations for being too broad, potentially sweeping in routine and benign business operations like inventory management and customer loyalty programs. These rules would impose heavy documentation and risk assessment burdens, discouraging businesses from offering useful services like personalized coupons. This would reduce competition, raise prices, and limit consumer choice.	The Agency disagrees with this comment. The regulations are clear about what technologies are in scope and are not overly expansive. Exercising its discretion, the Agency revised the regulations, including revising Article 11 to focus on the use of ADMT for a significant decision, to further simplify implementation for businesses at this time.
RAs / ADMT	1506	Comment recommends that the regulations should require that businesses document and justify all opt-out exceptions, not just the ADMT system's accuracy and non-discrimination, to strengthen enforcement.	The Agency disagrees with this comment. The Agency has revised the uses of ADMT that require a business to comply with Article 11's requirements to focus on the use of ADMT for significant decisions and accordingly revised the exceptions to when a business must provide an opt-out from its use of ADMT. These revisions balance protections for consumer privacy and simplify implementation for businesses at this time. With respect to the documentation requirements in § 7152(a)(6)(B), the Agency has revised the regulation so that a business is no longer required to document whether it evaluated the ADMT to ensure it works as intended for the business's proposed use and does not discriminate. The revised regulations include

			implementing policies, procedures, and training to ensure that the ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics as a safeguard that the business may consider. The Agency will continue to monitor the marketplace to determine whether modifications to the regulations are necessary.
RAs / ADMT	1522	Comment acknowledges that AI-based audio and video scoring systems may involve personal data and raise legitimate privacy risks depending on design. It supports a granular risk analysis to evaluate where on the risk scale any specific AI system falls.	The Agency agrees in part with this comment, to the extent it argues that certain uses of scoring systems present significant risk to consumers' privacy. If a business's use of scoring systems meets one of the thresholds in § 7150(b), the business must conduct a risk assessment. Additionally, exercising its discretion, the Agency deleted the definition of artificial intelligence as unnecessary. The CCPA and these regulations protect consumers' privacy and may apply to personal information processed by artificial intelligence whether stated expressly or not.
RAs / ADMT	1576	Comment recommends the Agency adopt a technology-neutral and principle-based regulatory framework rather than prescriptive classifications, such as those characterizing certain technologies or processing activities as presenting "significant risk." This would allow for flexibility as technologies evolve and enable businesses to meet regulatory goals through risk-based measures.	The Agency disagrees with this comment. It is unclear what the commenter means by technology-neutral. To the extent the commenter is requesting that the Agency remove regulations regarding ADMT, the Agency cannot do so. The Agency must issue regulations regarding opt-out and access rights with respect to businesses' use of ADMT, and regarding risk assessments for processing that presents significant risk to consumers' privacy.
RAs / ADMT	1579	Comment suggests the Agency ensure that the proposed regulations' use of "personal information" does not conflict with the CCPA's definition, which specifically excludes "publicly available information," unless the publicly available information is "biometric	The Agency disagrees with this comment. The regulations do not conflict with the CCPA's definition of "publicly available information." In addition, the CCPA's definition of "publicly available information" applies to

		information collected by a business about a consumer without the consumer's knowledge."	the regulations. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
RAs / ADMT	1582	Comment recommends assessing compliance based on demonstrable due diligence and good faith, as required by the CCPA.	The Agency agrees with this comment that compliance will be assessed consistent with the requirements of the CCPA. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
RAs / ADMT	1699	Comment recommends the Agency prioritize clarity around obligations under the statute over introducing new, additional obligations not expressly required by the law. Comment asserts that the Proposed Regulations exceed the statutory mandates of Civil Code §§ 1798.185(a)(14)-(15) by introducing unnecessarily detailed requirements.	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(14)-(15).) The regulations provide clarity and guidance regarding how to comply with the law, while providing flexible standards that are adaptable to a variety of use cases and contexts. However, the Agency has revised the regulations to simplify implementation for businesses at this time. The regulations balance protections for consumer privacy and flexibility for businesses.
RAs / ADMT	1700	Comment suggests the Agency provide flexibility where possible about how to comply with the law in a manner that prioritizes substance over form. Comment argues that inflexible and prescriptive requirements, such as elaborate "pre-use" notices and detailed checklists for risk assessments, will divert resources from substantive privacy programs.	The Agency disagrees with this comment to the extent that it suggests that the Pre-use Notice and risk assessment requirements are inflexible or unwarranted. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The Pre-use Notice requirements provide businesses with flexibility in how they are consolidated or included with the Notice at Collection while ensuring that consumers have meaningful information prior to exercising their CCPA rights. In addition, the Agency has revised the ADMT framework to focus on the use of ADMT for significant decisions to simplify implementation at this time. Regarding risk assessments, the regulations provide clarity and guidance regarding how to comply, while providing flexible standards that are adaptable to a variety of use

			cases and contexts. In addition, the regulations explicitly allow a business to use a risk assessment that it has prepared for another purpose, to comply with in § 7152. (*See* § 7156(b).) Therefore, to the extent a business is already complying with the risk assessment requirements in other laws, it can leverage those compliance processes to comply with the regulations. Further, the Agency has revised the regulations to simplify implementation for businesses at this time. The regulations balance protections for consumer privacy and flexibility for businesses.
RAs / ADMT	1701	Comment suggests the Agency align rules with existing national and global standards to facilitate consumer understanding and promote privacy-preserving business practices. Comment concerns that divergence from global and national privacy norms (e.g., GDPR, other state laws) and the proposed regulations' requirements that companies adopt California-specific notices, user choices, and risk assessment processes will increase compliance costs and confuse consumers.	The Agency disagrees with the comment. Although the Agency strives for consistency with privacy laws in other jurisdictions when appropriate, it must comply with California law and use its discretion to adopt requirements appropriate to California. Nevertheless, to simplify implementation for businesses at this time, the Agency modified the definition of ADMT to focus on a higher-risk use of ADMT at this time, which is a use without any human involvement. It also revised the definition of significant decision and § 7200, to focus on the use of ADMT for significant decisions. As revised, the regulations are consistent with approaches taken in other jurisdictions, such as the EU and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The Agency has determined that the regulations' requirements regarding notices, opt-out of ADMT, and risk assessments will not confuse consumers but will instead further protect their privacy. The proposed regulations are consistent with

			CCPA's direction to the Agency, and with its intent and purpose to further protect consumers' privacy.
RAs / ADMT	1746	Comment criticizes the lack of alignment between ADMT disclosures in risk assessments and Pre-use Notices. While both require an explanation of "logic," only Pre-use Notices require disclosure of "key parameters." Comment urges the Agency to clarify that businesses must identify in their risk assessment the key parameters that affect the output of a given ADMT, as well as any evidence that supports the relevance of those key parameters to the decision the business is ultimately attempting to make.	The Agency disagrees with this comment. The risk assessment requirements ensure that businesses identify the relevant logic of the ADMT, and how they will use the output of the ADMT to make a significant decision about a consumer. The Agency does not believe that additional information is necessary at this time.
RAs / ADMT	1803	Comment recommends being able to request a signed Data Processing Agreement with every organization that holds the consumer's personal information, which the consumer can try to enforce without any assistance from enforcement agencies. Comment notes that very few organizations will provide such a Data Processing Agreements unless a consumer is a paying customer.	While not on the proposed action, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
RAs / ADMT	2052, 2053, 2054	Comment argues the proposed rules should consider all uses of generative AI and LLMs to collect and process data, not just to train other AI models. Generative AI and LLM systems are especially risky because they are prone to degradation after successful initial implementation. Comment argues it has remained difficult validating the outputs generated by generative AI and LLM systems.	The Agency agrees with this comment to the extent it supports safeguards for consumers' privacy as businesses use ADMT. With respect to AI, exercising its discretion, the Agency has also revised the regulation to remove references to AI as unnecessary. The CCPA and these regulations protect consumers' privacy and may apply to personal information processed by artificial intelligence whether stated expressly or not.

ARTICLE 12. INSURANCE COMPANIES

Section of Regulation	Comment Numbers	Summary of Comments 45-Day Comment Period	Agency Response
Insurance	375	Comment objects to defining insurance companies based on the California Insurance Code while requiring them to comply with CCPA for non-insurance-related personal data. Comment requests deletion of language suggesting this dual compliance obligation.	The Agency disagrees with this comment. § 7271(a) clarifies the definition of "insurance companies" and does not impose a dual compliance obligation. The regulations do not require insurance companies to comply for data processed "in connection with insurance transactions" as specified in Insurance Code, § 791.02. Rather, the regulations apply only to personal information collected or processed for purposes outside of an insurance transaction. The definition is included to clarify which businesses are subject to the regulations, ensuring appropriate compliance without extending its scope beyond what is intended.
Insurance	384, 385, 394, 395, 699, 799, 1137, 1141, 1142, 2014, 2015, 2016	Comment appreciates the Agency's stated intent to set a baseline for regulations governing the insurance industry and the recognition that insurers already have existing privacy obligations under the IIPPA, but questions if it is truly necessary and if now is the correct time to proceed with the rulemaking. Insurers are already subject to robust legal and regulatory framework at both the state and national levels (e.g., GLBA, FCRA, HIPAA), enforced by the Insurance Commissioner to protect consumer rights. In CA, they are subject to the Insurance Information and Privacy Protection Act (IIPPA), as well as strict anti-discrimination and other privacy laws (e.g., CDI Bulletin 2022-5). Consumers who share their personal information with insurance companies are already protected regardless of what the Agency does. The Agency's regulations do not	The Agency disagrees with this comment. Civil Code § 1798.185(a)(20) requires the Agency to adopt regulations applying the parts of the CCPA that are more privacy protective than the insurance code to insurance companies. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. These regulations are necessary to address any ambiguity regarding insurance companies' obligations under the CCPA. These regulations acknowledge that the CCPA and Insurance Code may overlap in their jurisdiction and delineate the boundary between the two legal frameworks. In addition, Articles 9-11 are meant to be robust and applicable to many factual situations and across industries. Those regulations are consistent with approaches taken in other jurisdictions, such as GDPR and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses.

		meaningfully enhance consumer privacy or provide clear benefits to insurance consumers; instead, they introduce unnecessary complexity and regulatory friction in an already well-regulated sector. The Agency should inject clarity and certainty for both consumers and industry. To avoid confusion and redundancy, the Agency should align its rules with existing laws and ongoing regulatory updates and wait for the National Association of Insurance Commissioners (NAIC) to complete its model law revisions. Specifically, Articles 9, 10, and 11 should be revised to better integrate with established industry standards and compliance frameworks or deleted because they are unnecessary and duplicative.	
Insurance	386, 700, 800, 1134, 1135, 1136	Comment suggests that § 7271(a) in the regulations does not properly account for the CCPA exemptions (e.g., GLBA, CFIPA, HIPAA, FCRA) and could mistakenly bring already-exempt insurance data under the CCPA. Comment also finds the example to be confusing and misleading. Comment requests amendment of § 7271(a) to clarify that only data not covered by IIPPA or CCPA exemptions is subject to CCPA. Alternatively, the Agency should provide guidance rather than a rulemaking.	The Agency disagrees with this comment. These insurance regulations clarify existing requirements under the CCPA and respond to concerns regarding the personal information collected, used, processed, or retained by insurance companies that are not subject to the Insurance Code and other laws, such as the federal Gramm-Leach-Bliley Act. They do not introduce new laws, nor amend existing legal rights or requirements. Nevertheless, the Agency has added a counterexample to demonstrate an instance where information covered by the Insurance Code is not subject to the CCPA. Additionally, the Agency must use rulemaking to establish requirements related to the applicability of CCPA to insurers in accordance with the Administrative Procedure Act.
Insurance	702	There is no assumption that a regulation must be adopted, only that the Agency conduct an analysis of the relevant laws and if it identifies	The Agency disagrees with this comment. The Agency has analyzed the difference between insurance laws and the CCPA. These regulations clarify existing requirements under

		areas where CCPA provides greater protections, then to develop regulations that apply those greater protections to insurance providers. The Agency has put the cart before the horse by proposing regulations before conducting the required analysis. This is particularly problematic given the changes to insurance privacy laws that are likely to go into effect. The Agency should refrain until there's more clarity as to efforts on the NAIC front.	the CCPA and respond to concerns regarding the personal information collected, used, processed, or retained by insurance companies that are not subject to the Insurance Code and other laws, such as the federal Gramm-Leach-Bliley Act. Commenter misconstrues the plain language of the regulations.
Insurance	703	In defining "insurance companies" in § 7270, referencing the California Insurance Code generally is too broad. There are many entities subject to the Insurance Code that are not what would traditionally be considered "insurance companies" and yet are otherwise covered by GLBA, the IIPPA, and the PNPI rules. The regulations should be scoped specifically to entities that are subject to IIPPA. Additionally, "insurance company" should include any entity that is controlled by and shares common branding with the insurance company.	The Agency disagrees with this comment. These regulations set the baseline for the insurance industry. They clarify that that those entities subject to insurance laws that also meet the definition of "business" under the CCPA are to comply with the CCPA with regard to personal information that is not subject to those insurance laws. Narrowing the definition as the commenter proposes is not as effective in clarifying how the CCPA applies to the insurance industry. Moreover, the Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
Insurance	704	§ 7271(a) delineating between personal information subject to CCPA and personal information "subject to the Insurance Code" likewise could be further clarified, and the example provided in the regulations definitions should be removed or moved to the section with other examples. Also, the second sentence should be deleted.	The Agency does not agree with this comment. The regulation is reasonably clear, and the examples provided adequately explain what is meant by personal information that is subject to the Insurance Code. Moreover, the Agency has added a counterexample to demonstrate an instance where information covered by the Insurance Code is not subject to the CCPA. The comment does not provide a reason why the second sentence should be deleted. The Agency believes it is necessary to clarify what is meant by information subject to the Insurance Code.

Insurance	801	Comment supports § 7271(a), which it interprets as recognizing the exclusive authority of the CDI as it relates to the oversight and regulation of ratemaking and the operation of insurance policies.	The Agency agrees in part with this comment and notes commenter's support. The CDI has oversight over insurance companies; however, insurance companies may also be subject to laws falling within the authority of other government agencies as they engage in business activities.
Insurance	705	The Agency should reconsider the examples in § 7271(b). While employment-related information of employees of insurance companies is not subject to GLBA or IIPPA, and therefore is subject to the CCPA, data collected from website visitors may be subject to IIPPA or GLBA. Whether a website visitor is a "customer" or "consumer" under the GLBA, and therefore whether their personal information would be subject to the GLBA rather than the CCPA, is a much more nuanced analysis than the example suggests. Instead, the Agency could include as an example instances where an insurance company's use of non-public personal information subject to IIPPA, GLBA, or PNPI would not be subject to the Agency's requirements, such as those regarding automated decision-making tools. At a minimum, the Agency should consult the California Department of Insurance on how to properly draw the line between GLBA and CCPA domains, including with respect to personal information collected by website cookies. The Agency should also add an example that PI collected for the purposes of workers' compensation insurance is not subject to the CCPA.	The Agency does not agree with this comment. The Agency has been in contact with the CA Department of Insurance throughout the rulemaking process. The examples provided adequately demonstrate where the CCPA's jurisdiction begins and the Insurance Code's jurisdiction ends. The comment does not explain how the data collected from website visitors would be subject to the IIPPA or GLBA, especially in light of language in the example that says the visitors have not applied for any insurance product or other financial product or service. Moreover, the Agency has added a counterexample to demonstrate an instance where information covered by the Insurance Code is not subject to the CCPA. The Agency does not believe that the commenter's example about workers' compensation insurance is necessary at this time.
Insurance	706	The Agency should consider adding explicit language in § 7271(a) that the likelihood of successor legislation will enhance and further	The Agency disagrees with this comment. These insurance regulations clarify existing requirements under the CCPA and respond to concerns regarding personal information

		clarify current law. Accounting for that likelihood now would not foreclose the Agency's ability to review any new legislation in the context of its responsibilities under CCPA, but it does provide industry with some certainty and predictability by establishing a default position for the regulations through any new statutes.	collected, used, processed, or retained by insurance companies that are not subject to the Insurance Code or other laws, such as the federal Gramm-Leach-Bliley Act. They do not introduce new laws, nor amend existing legal rights or requirements. Moreover, commenter's proposed language of referring to successor legislation does not comply with the APA's clarity standards.
Insurance	698	Comment proposes adding § 7271(b) to explicitly regulate how insurance companies handle device-generated data (e.g., telematics and wearables). Without clear language, insurers may incorrectly claim exemptions for device-generated data that is not directly tied to underwriting or claims processes.	The Agency disagrees in part with this comment. The Agency has determined that this language is not necessary at this time. Whether this kind of data is subject to the CCPA is a fact-specific analysis.
Insurance	701	Comment expresses concern over the Agency's bundling of insurance regulations with cybersecurity audits, risk assessments, and automated decision-making regulations. The entire package manifests unreasonable overreach that will impose significant burdens and uncertainty on industry and innovation, with no material improvement to consumer privacy or the protection of consumer personal information. The Agency should address each topic separately to ensure that it has given itself and the public sufficient opportunity to consider the best path forward on each set of proposals.	The Agency disagrees with this comment. As an initial matter, the regulations are within the Agency's authority and further the intent and purpose of the CCPA, as amended by the California Privacy Rights Act, which California voters overwhelmingly supported via passage of Proposition 24 in 2020. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security to perform a thorough and independent annual cybersecurity audit. The CCPA also directs the Agency to require businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment and submit it to the Agency on a regular basis. (Civ. Code § 1798.185(a)(14).) The CCPA further directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The CCPA also directs the Agency to review certain Insurance Code provisions and regulations relating to consumer privacy and

			then issue regulations applying the more privacy protective provisions of the CCPA to insurance companies. (*See* Civ. Code § 1798.185(a)(20).) The Agency has separately addressed each topic within the rulemaking package. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, it is required to issue regulations and impose certain requirements on these topics. Also, the Agency has appropriately considered the impact on businesses and innovation and has made efforts to limit the burden of the regulations while implementing the CCPA. The Agency engaged in robust preliminary and formal rulemaking activities with a wide variety of stakeholders and has collaborated with state lawmakers and will continue to do so, consistent with the CCPA's direction to the Agency. (*See* Civ. Code § 1798.199.40(g).) The resulting regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Nevertheless, the Agency has modified the regulations to significantly reduce their costs.

ARTICLE 13. INVESTIGATIONS AND ENFORCEMENT

Section of Regulation	Comment Numbers	Summary of Comments 45-Day Comment Period	Agency Response
7302(e)	909	Comment argues that the regulation removes language ensuring that probable cause determinations are not admissible in court proceedings. Comment requests reinstating this protection.	The Agency disagrees with this comment. The revision was necessary to avoid the misimpression that these regulations amend the rules of evidence. The Agency does not have the authority to change the rules of evidence for court proceedings.
Enforcement	263, 601, 902, 1015, 1304,	Comment argues that given the breadth and scope of the updates to existing CCPA regulations, cybersecurity audit requirements,	The Agency disagrees in part with this comment. The CCPA clearly states that the enforcement of regulations is based on the effective date. The Agency cannot amend the CCPA

	1306, 1402, 1476, 1491, 1761, 1982, 1985	and new ADMT rules, the Agency should clarify that civil and administrative enforcement of new regulatory provisions will not commence until one year from the date the provisions are in effect. Comment argues that the timeline for the regulations is too aggressive and the Agency should allow businesses a reasonable time to comply with any new regulations. The complexity and novelty of these regulations will require businesses to develop and implement technical solutions that will take time and significant resources to develop and operationalize. As such, comment requests a minimum 24-month implementation period for the regulations. Comment asserts that the Agency should make clear that the requirements apply to processing activities created or generated after December 31, 2026, only and are not retroactive to any processing activities created or generated before January 1, 2027.	or adopt regulations inconsistent with it. The regulations are also clear with respect to the processing activities they apply to. The Agency believes that no further clarification is needed at this time. As to timing to implement the new regulations, the Agency agrees in part with this comment. The regulations have been revised to provide additional time for compliance to simplify implementation for businesses at this time. The regulations have been modified to include a three-year phased implementation for cybersecurity audits. The submission requirements for both cybersecurity audit certifications and risk assessment information have been simplified and the deadline to complete initial submissions has been extended to April 1, 2028. Regarding ADMT requirements, the Agency has revised § 7200(b) to provide a specific date, January 1, 2027, by which a business must be in compliance with the requirements.
Enforcement	1146, 1150, 1259	Comment argues that the regulations do not adhere to the required one-year gap between adoption and enforcement, which is crucial for businesses to prepare for compliance. Immediate enforcement would disproportionately burden small businesses with limited resources. Comment urges the Agency to provide a full 12-month compliance period after final regulations are adopted to give businesses sufficient time to adapt. The Agency's immediate implementation timeline gives businesses no time to comply, leading to rushed or abandoned ADMT adoption. This could lead businesses to abandon ADMT tools that enhance equity in decision-making.	The Agency disagrees with the comment's interpretation of the CCPA. The CCPA does not require a one-year gap between adoption and enforcement. Nevertheless, the regulations have been revised to provide additional time for compliance to simplify implementation for businesses at this time. The regulations have been modified to include a three-year phased implementation for cybersecurity audits. The submission requirements for both cybersecurity audit certifications and risk assessment information have been simplified and the deadline to complete initial submissions has been extended to April 1, 2028. Regarding ADMT requirements, the Agency has revised § 7200(b) to provide a specific date, January 1, 2027, by which a business must be in compliance with the requirements. The regulations

		Further, the lack of compliance flexibility discourages innovation and undermines AI's potential benefits.	balance providing privacy protections for consumers with flexibility for businesses to come into compliance. They also have been revised to further simplify implementation for businesses at this time.

OTHER TOPICS – COSTS

Section of Regulation	Comment Numbers	Summary of Comments 45-Day Comment Period	Agency Response
Costs	2, 21,127, 206, 214, 332, 426, 427, 430, 456, 461, 464, 467, 476, 479, 508, 513, 532, 533, 1189, 1244, 1249, 1287, 1288, 1977, 1990, 2026, 2037, 2041	Comment states the regulations would impose unnecessary costs totaling $31 billion, with significant economic impacts including job losses and reduced state GDP, while offering no additional privacy benefits beyond existing regulations. Comment believes the Agency is overstepping its authority. Comment claims that the regulations go beyond privacy and security concerns, which contradicts Proposition 24's intent to balance privacy protections with business and innovation. The Agency creates an expansive regulatory framework that applies even to routine business technologies, leading to massive compliance costs for businesses. They regulate widely used, longstanding business tools rather than focusing on true AI systems that make autonomous decisions imposes unnecessary compliance burdens. § (3)(C)(1) mandates that consumer rights and business responsibilities be	The Agency disagrees with this comment. As an initial matter, the regulations are within the Agency's authority and further the intent and purpose of the CCPA, as amended by the California Privacy Rights Act, which California voters overwhelmingly supported via passage of Proposition 24 in 2020. The law directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security to perform a thorough and independent annual cybersecurity audit. The CCPA also directs the Agency to require businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment and submit it to the Agency on a regular basis. (Civ. Code § 1798.185(a)(14).) The CCPA further directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, it is required to issue regulations and impose certain requirements on these topics. Also, the Agency has appropriately considered the impact on businesses and innovation and has made efforts to limit the burden of the regulations while implementing the CCPA. The Agency engaged in robust preliminary and formal rulemaking activities with a wide variety of stakeholders and has collaborated with state lawmakers and will continue to do so, consistent with the CCPA's direction to the Agency. (*See* Civ. Code § 1798.199.40(g).) The resulting regulations will

		implemented while considering their impact on businesses and innovation. However, the SRIA indicates that the regulations will have significant and irreversible economic consequences. Given the projected $2 billion budget deficit in 2025, comment argues that the regulations could worsen the state's financial situation. It may drive businesses out of CA. The regulations fail the consistency standard under Government Code § 11349(d), which requires that regulations not conflict with existing statutes or legal provisions. They represent an existential threat to CA's business environment.	generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Nevertheless, the Agency has modified the regulations to significantly reduce their costs. For example, the Agency revised the regulations to phase in the cybersecurity audit requirements over three years, which contributes favorably to the State's current budget situation. Direct costs over 10 years have decreased from $9.7 billion to $6.9 billion and overall quantifiable benefits have increased from $186 billion to $282 billion. The number of jobs lost in the first year also decreased and the number of jobs created over 10 years increased from 233,000 to 348,000. The gross state product in the 10th year also increased from $290 billion to $369 billion.
Costs	4, 7, 16, 20, 23, 33, 37, 41, 47, 48, 55, 58, 63, 65, 69, 120, 128, 218, 333, 454, 457, 482, 539, 541, 552, 560, 564, 565, 568, 765, 1014, 1061, 1064,	Comment states the regulations impose a disproportionate financial burden and long-term financial strain on small and mid-sized businesses compared to larger corporations. They burden businesses with unnecessary compliance costs without delivering meaningful privacy benefits. The CA Department of Finance's Economic and Fiscal Impact Statement estimates that compliance will cost each small business $20,000 annually for a decade. The regulations exacerbate untenable compliance costs for small businesses and potentially lead to job losses and lost sales. It could force smaller companies out of the market or out of the state, favoring larger	The Agency disagrees with this comment. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The regulations are consistent with the Agency's mandate under, and the requirements of, the CCPA. The regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Moreover, most of the costs of the regulations fall on larger businesses dealing with a large amount of personal information and with annual revenues that are greater than $28 million. Additionally, the Delete Act is a separate law and only applies to data brokers, not all businesses subject to the CCPA. Nevertheless, the Agency has modified the regulations to significantly reduce their costs on small businesses. The range of first year costs for small businesses has decreased from $7,045 – $92,896 to $6,058 – $36,950. Also, most costs associated with obtaining technical and legal advice are attributed to the regulatory baseline, and thus, appropriately not included in the SRIA. (*See* SRIA, pp. 20-21.) Moreover, the Agency recognizes in the SRIA that not every cost can

	1148, 1238, 1240, 1534, 1646, 1648, 1739, 1742, 1947, 1960, 1963, 1992	corporations with more resources. Small businesses lack resources to navigate a complex regulatory environment. Small businesses are already dealing with inflation and supply chain disruptions. They lack the financial flexibility to absorb such drastic regulatory changes. It's especially hard for those businesses dealing with increases in fees under the Delete Act. Additional costs for legal and technical compliance were not fully accounted for in the impact statement. Moving forward with the rulemaking despite this foreseeable harm undermines the intent of Proposition 24.	be estimated, which is why the Agency took a more general approach and focused on the areas that it expects to have the highest costs. Costs to consumers and the California economy at large are reflected in the Agency's macroeconomic impact estimates.
Costs	208, 210, 211, 1261, 1575, 1894	Comment argues that businesses, especially small and mid-sized ones, would face excessive regulatory burdens, including mandatory risk assessments, audits, and consumer opt-out requirements, even for low-risk, widely accepted business practices. The SRIA does not account for the effect on the ongoing use or adoption of AI, and the benefits that businesses seek to achieve through the use of AI. These businesses may struggle to adapt and remain competitive. They may also negatively impact the supply chain or small business recovery for those who are trying to rebuild after emergencies like the recent wildfires in LA County. The estimated cost of compliance —	The Agency disagrees with this comment. The regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. The Agency has made a good faith effort to estimate the costs associated with these regulations. Moreover, most of the costs of the regulations fall on larger businesses dealing with a large amount of personal information and with annual revenues that are greater than $28 million. Further, respecting consumer privacy and data protection is not contrary to innovation and entrepreneurship; rather, the regulations foster the development of privacy-by-design products and services. Nevertheless, the Agency has modified the regulations to significantly reduce their costs, including for small businesses. References to artificial intelligence have been removed to simplify implementation at this time. Direct costs over 10 years have decreased from $9.7 billion to $6.9 billion and overall quantifiable benefits have increased from $186 billion to $282 billion. The number of jobs lost in the first year also decreased and the number of jobs created over 10 years increased from 233,000 to 348,000. The range

		$3.5 billion — is likely an understatement. Comment urges a thoughtful reconsideration of these regulations to ensure they protect consumers without unduly burdening businesses or stifling innovation.	of first year costs for small businesses has decreased from $7,045 – $92,896 to $6,058 – $36,950. The gross state product in the 10th year also increased from $290 billion to $369 billion. Regarding the comment's claim that the costs are an understatement, the Agency has made a good faith effort to estimate the costs associated with these regulations. The comment does not provide any specificity to explain why they think the cost is an understatement.
Costs	520, 769, 1649	Comment recommends that the Agency to conduct a comprehensive economic impact analysis to better understand the burdens on small and minority-owned businesses. Comment points out that AAPI small businesses often lack internal capacity for compliance and face language and cultural barriers, which make the ADMT requirements even harder to meet.	The Agency disagrees with this comment. The Agency has already analyzed the economic impact of the regulations on small businesses, which would include minority-owned small businesses, and has modified the regulations to significantly reduce the costs of the regulations on small businesses. The regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Moreover, most of the costs of the regulations fall on larger businesses dealing with a large amount of personal information and with annual revenues that are greater than $28 million. Also, most costs associated with obtaining technical and legal advice are attributed to the regulatory baseline, and thus, appropriately not included in the SRIA. (*See* SRIA, pp. 20-21.) Moreover, the Agency recognizes in the SRIA that not every cost can be estimated, which is why the Agency took a more general approach and focused on the areas that it expects to have the highest costs. Costs to consumers and the California economy at large are reflected in the Agency's macroeconomic impact estimates. Nevertheless, the Agency has modified the regulations to significantly reduce their costs on small businesses. The range of first year costs for small businesses has decreased from $7,045 – $92,896 to $6,058 – $36,950.
Costs	544, 633, 1245, 1326, 1387,	Comment critiques the Agency's economic impact analysis, suggesting it underestimates implementation costs. Comment argues that it underestimates the number of businesses affected by	The Agency disagrees with this comment. The impact of the regulations on foreign businesses and businesses in other states without a physical presence in CA are outside the scope of the SRIA. Government Code § 11346.3(a) requires the SRIA to look at the regulation's impacts on California business enterprises. According to

	2008, 2020	only including businesses with employees in CA and eschewing out-of-state companies that sell into CA and its markets. It does not account for increased costs because of the reduction in competition because out-of-state businesses will be incentivized to leave the CA market. It also does not consider the regulations' costs on ongoing operating costs and productivity, such as those related to intake/response to ADMT requests, administering a non-automated process for each ADMT-covered decision, responding to ADMT requests, and the negative impact of opt-outs on the reliability of ADMT or behavioral advertising. The Agency also does not account for new California businesses that will come under the scope of the CCPA as they grow in revenue or size. The CPPA should update the SRIA to: (1) reflect the impact on out-of-state businesses that are nonetheless subject to the statutory requirements; (2) accurately reflect operational costs of cybersecurity audits and risk assessments; (3) account for the significant technical and operational burden of ADMT opt-out and access rights; (4) reflect the impact on businesses related to the suppression of behavioral advertising; and (5) address elements required under	the California Employment Development Department methodology, this means firms with a physical presence in CA. The Agency has made a good faith effort to estimate the costs associated with these regulations on businesses with a physical presence in CA. While increased regulations could lead to decreased investment and jobs, the CA market is too significant for businesses that span state or country lines to ignore. The Agency does not believe that those businesses will not exit the California market entirely especially because many of these regulatory costs are coming or already exist in other jurisdictions. A global or US-wide company will have to meet similar regulatory requirements in other markets. Also, the Agency recognizes in the SRIA that not every cost can be estimated, which is why the Agency took a more general approach and focused on the areas that it expects to have the highest costs. The Agency made a good faith effort to estimate the costs associated with these regulations given available data. Costs to consumers and the California economy at large are reflected in the Agency's macroeconomic impact estimates. As to businesses that will come under the scope of the CCPA as they grow in revenue or size, the Agency reasonably assumes that the number of companies in this category is likely small and including them will not significantly affect the main takeaways of the economic assessment. Further, the Agency captured some costs to new businesses in its assessment of ongoing costs. Finally, the regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Nevertheless, the Agency has modified the regulations, including removal of the behavioral advertising threshold, to significantly reduce the costs of the regulations.

		California law, including an evaluation of the Draft Regulations' impact on "the incentives for innovation in products, materials, or processes." The burden of the regulations exceeds their utility.	
Costs	299	Benefits are likely overestimated and protections against discriminatory outcomes for most categories of "significant decisions" already exist in state consumer protection and federal civil rights laws. Many costs may be missing from these estimates. Direct and opportunity costs may shorten the lifespan of startups and divert resources from necessary startup activities like product development and customer acquisition. Costs are not just limited to California businesses. They will accrue to any business or startup across the US selling to or wanting to sell to the CA market and those costs should be accounted for.	The Agency disagrees with this comment. The benefits are actually underestimated because the vast majority of expected benefits cannot be quantified. They are not just related to discriminatory outcomes, but improvements to the health, safety, welfare, and quality of life for Californians. Also, protections related to already existing state consumer protection and federal civil rights laws were not attributed to the regulation. Regarding lost opportunity costs and the related impact on business growth, the Agency recognizes in the SRIA that not every cost can be estimated, which is why the Agency took a more general approach and focused on the areas that it expects to have the highest costs. Costs to consumers and the California economy at large are reflected in the Agency's macroeconomic impact estimates. Further, costs are likely overestimated because initially the Agency made conservative estimates regarding the number of firms affected. Regarding costs to out-of-state businesses, the impact of the regulations on foreign businesses and businesses in other states without a physical presence in CA are outside the scope of the SRIA. Government Code § 11346.3(a) requires the SRIA to look at the regulation's impacts on California business enterprises. According to the California Employment Development Department methodology, this means firms with a physical presence in CA. The Agency has made a good faith effort to estimate the costs associated with these regulations on businesses with a physical presence in CA.
Costs	306, 484, 1144, 1389, 1469, 1470	Comment states that the regulations do not benefit consumers because it undermines online advertising and degrades the customer experience. Advertising alerts consumers to better	The Agency disagrees with this comment. The Agency made a good faith effort to estimate the costs associated with these regulations. The regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Moreover, most of the costs of the

		deals, products they are interested in, and help make service affordable or lower cost. The SRIA ignores the revenue impacts of the regulations, including costs related to the suppression of behavioral advertising. The SRIA fails to reflect the breadth of these activities and overlooks the scope of the impact and true costs on businesses who may have to scale back or eliminate this kind of commonplace advertising. It also does not address the impact on consumers who will receive fewer offers and promotions for products and services that are most likely to be valuable to them. The regulations cost $3.4 billion while affecting 52,326 businesses. They will make CA businesses less competitive compared to out-of-state competitors and will drive businesses out of state. Small businesses and taxpayers can't afford such destructive regulations.	regulations fall on larger businesses dealing with a large amount of personal information and with annual revenues that are greater than $28 million. Nevertheless, the Agency modified the regulations to significantly reduce the costs of the regulations, including for small businesses. Specifically, it revised the regulations to remove the profiling for behavioral advertising threshold.
Costs	1009	Comment asserts that the ADMT regulations will dramatically increase the cost and complexity of digital advertising. To survive, many small businesses will simply pass cost increases on to consumers at a time when many American households are reeling from today's inflationary economy. They would also restrict consumer choices.	The Agency disagrees with this comment. The regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Moreover, most of the costs of the regulations fall on larger businesses dealing with a large amount of personal information and with annual revenues that are greater than $28 million. Nevertheless, the Agency modified the regulations to significantly reduce the costs of the regulations, including for small businesses. Specifically, it revised the regulations to remove the profiling for behavioral advertising threshold. Also, regarding pass-through costs, the Agency recognizes in the SRIA that not every cost can be

			estimated, which is why the Agency took a more general approach and focused on the areas that it expects to have the highest costs. Costs to consumers and the California economy at large are reflected in the Agency's macroeconomic impact estimates.
Costs	1260	Comment expresses concerns about the ADMT regulations, arguing that while privacy protection is important, the rules would significantly increase compliance costs for businesses. These costs would ultimately be passed on to consumers while also restricting consumer choice.	The Agency disagrees with this comment. The regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Nevertheless, the Agency has revised the definitions of ADMT and significant decision to focus on a higher-risk use of ADMT. The revised definition of ADMT focuses on uses without any human involvement and the revised definition of "significant decision" no longer includes the phrase "access to." As revised, the regulations are consistent with approaches taken in other jurisdictions, such as GDPR and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. This balances protections for consumer privacy and simplifying implementation for businesses at this time. Regarding the suggestion that the regulations restrict consumer choice, the comment does not provide support for how the regulations restrict consumer choice. The regulations expand consumers' choices and control with respect to businesses' use of ADMT.
Costs	21, 30, 38, 49, 56, 66	Comment states upgrading security infrastructure to meet new standards could cost thousands, diverting resources from reinvestment in the business and employees. The cybersecurity audit requirements may also divert already scarce privacy and cybersecurity resources toward administrative compliance. This dynamic reduces businesses' ability to invest in proactive security measures, leaving them more vulnerable to	The Agency disagrees with this comment. The commenter claims that the regulations require them to update security infrastructure to meet the new standards, but the requirement to implement reasonable security procedures and practices has been in the law since 2004 and is reinforced in the CCPA. (*See* Civ. Code §§ 1798.81.5(b) and 1798.100(e).) These regulations do not address upgrading security infrastructure which businesses should have already been doing. Further, the regulations help to assure that businesses are allocating proper resources to cybersecurity to protect consumers' personal information. While the Agency acknowledges that the regulatory requirements will take time and resources, the regulations implement requirements mandated by the CCPA. The Agency cannot amend the

		cyberattacks. This directly undermines the objectives of the statutory requirement for a cybersecurity audit.	CCPA or adopt regulations inconsistent with the CCPA. Nevertheless, the Agency has modified the regulations to significantly reduce their costs.
Costs	24, 42, 51, 59, 70, 130, 133, 296, 475, 511, 522, 551, 569, 570, 661, 771, 1147, 1175, 1263, 1480, 1650, 1664, 1740, 1955, 1959, 1984, 1993, 2024, 2029	Comment suggests that while business owners respect consumer privacy and data protection, compliance shouldn't come at the cost of entrepreneurship, or the adoption of modern technologies like AI. The regulations will hinder CA's economic growth and stifle innovation, including in areas like AI and machine learning. They will slow technological progress, create compliance challenges exceeding European regulations, cause notice fatigue, and cause unnecessary consumer confusion through excessive disclosures. ADMT-related pop-ups will make it hard for consumers to navigate and drive traffic to non-CA competitors from small businesses. They fall short of consumer protection goals and can be counterproductive because people often click "yes" (or "no") to everything without paying attention. Comment cites examples regarding pop-ups and notices that would impede consumers and cause unnecessary friction without improving consumer understanding. The need to continually update risk assessments and disclosures, even for minor system changes, may delay or avoid unnecessary improvements and innovation. Also, the required transparency measures might force	The Agency disagrees with this comment. Respecting consumer privacy and data protection is not contrary to innovation and entrepreneurship; rather, the regulations foster the development of privacy-by-design products and services. The Agency has appropriately considered the impact on businesses and innovation. The ADMT, cybersecurity audit, and risk assessment regulations balance providing protections for consumers' privacy while providing flexibility businesses to come into compliance. Moreover, the regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. With respect to consumer notices, the notice requirements provide businesses with flexibility in how they are consolidated or included with the Notice at Collection. The Agency disagrees that the notice requirements would impede consumers, because these notices ensure that consumers have meaningful information prior to exercising their CCPA rights. As for trade secrets, the comment does not provide support for how the information required to be provided would include trade secrets or pose security risks. As for risk assessments, requirements to update risk assessments and submissions are necessary to ensure that risk assessments address risks to consumers' privacy throughout a processing activity's lifecycle and do not reflect out-of-date information. Nevertheless, the Agency has modified the regulations to significantly reduce their costs and simplify implementation for businesses, including small businesses, at this time. The Agency specifically exempts the disclosure of trade secrets and certain information related to security, fraud prevention, or safety from inclusion in the Pre-use Notice and the information provided to consumers in response to a request to access ADMT. (*See* §§ 7220(d), 7222(c).) The Agency also removed references to AI in its discretion.

		businesses to disclose trade secrets, harming competition and enabling fraudsters to exploit security systems. All this will push CA businesses to innovate elsewhere, ultimately impacting CA's competitive edge. Comment recommends that the Agency review the notice requirements and eliminate individualized notices for anything other than true high risk activities. Similarly, the comment argues that the cybersecurity audit and risk assessment regulations are more burdensome than necessary.	
Costs	321, 424, 766	Comment argues that California's leadership in technology and innovation is at risk due to overly broad and undefined regulatory scope. Specifically, the proposed regulations on ADMT and AI risk assessments will undermine California's leadership in the technology sector. Regulations affecting "access and provision" of data will introduce uncertainty and high compliance costs, discouraging businesses from testing new algorithms and technologies in the state.	The Agency disagrees with the comment. Respecting consumer privacy and data protection is not contrary to innovation and entrepreneurship; rather, the regulations foster the development of privacy-by-design products and services. The regulations are consistent with the CCPA's direction to the Agency with respect to ADMT, and with the CCPA's intent and purpose to further protect consumers' privacy while giving attention to the impact on business and innovation. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The regulations have also been revised to further simplify implementation for businesses at this time. The Agency revised the definitions of ADMT and significant decision to focus on a higher-risk use of ADMT. The revised definition of ADMT focuses on uses without any human involvement and the revised definition of "significant decision" no longer includes the phrase "access to." As revised, the regulations are consistent with approaches taken in other jurisdictions, such as GDPR and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. This balances

			protections for consumer privacy and simplifies implementation for businesses at this time.
Costs	1394, 1211	The SRIA should satisfy all of the requirements under CA law, including the prognosis on CA innovation, and to align with the ballot initiative's direction to the CPPA to "balance the goals of strengthening consumer privacy while giving attention to the impact on businesses." Governor Newsom has consistently emphasized the need to "maintain [California's] dominance" and "maintain [Californian] innovation." However, the regulations' broad applicability, prescriptive and granular requirements, and inflexibility would stifle ADMT development and technological innovation in California, as well as burden consumers through numerous and confusing notices and opt-out choices. The ADMT regulations should impose the same standards as those enacted under other consumer privacy frameworks to avoid putting CA businesses at a regulatory disadvantage.	The Agency disagrees with the comment. Respecting consumer privacy and data protection is not contrary to innovation and entrepreneurship; rather, the regulations foster the development of privacy-by-design products and services. The regulations are consistent with the CCPA's direction to the Agency with respect to ADMT, and with the CCPA's intent and purpose to further protect consumers' privacy while giving attention to the impact on business and innovation. Nevertheless, the Agency has revised the definitions of ADMT and significant decision to focus on a higher-risk use of ADMT. The revised definition of ADMT focuses on uses without any human involvement and the revised definition of "significant decision" no longer includes the phrase "access to." As revised, the regulations are consistent with approaches taken in other jurisdictions, such as GDPR and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. The Agency has also revised the Pre-use Notice requirements and the exceptions to when a business must provide an opt-out from its use of ADMT, which includes providing businesses with flexibility in how they consolidate or include the Pre-Use Notice with the Notice at Collection. The Pre-use Notice ensures that consumers have meaningful information prior to exercising their CCPA rights, and the opt-out provisions ensure that consumers can effectuate their right to opt-out of ADMT. These revisions balance protections for consumer privacy and simplifying implementation for businesses at this time.
Costs	1921	These regulations could cost up to $1.4 billion per the CPPA's own analysis, with little demonstrated value to consumers. It should adopt a more targeted approach like Colorado's, focusing on significant, fully automated decisions. It ignores § 3 of the CPRA that directs the	The Agency disagrees with this comment. As an initial matter, the regulations are within the Agency's authority and further the intent and purpose of the CCPA, as amended by the California Privacy Rights Act, which California voters overwhelmingly supported via passage of Proposition 24 in 2020. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security

		Agency to give attention to the impact on business and innovation and to assist businesses with compliance.	to perform a thorough and independent annual cybersecurity audit. The CCPA also directs the Agency to require businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment and submit it to the Agency on a regular basis. (Civ. Code § 1798.185(a)(14).) The CCPA further directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, it is required to issue regulations and impose certain requirements on these topics. Also, the Agency has appropriately considered the impact on businesses and innovation and has made efforts to limit the burden of the regulations while implementing the CCPA. The Agency engaged in robust preliminary and formal rulemaking activities with a wide variety of stakeholders and has collaborated with state lawmakers and will continue to do so, consistent with the CCPA's direction to the Agency. (*See* Civ. Code § 1798.199.40(g).) The resulting regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Nevertheless, the Agency has modified the regulations to significantly reduce their costs. For example, the Agency revised the definitions of ADMT and significant decision to focus on a higher-risk use of ADMT. The revised definition of ADMT focuses on uses without any human involvement and the revised definition of "significant decision" no longer includes the phrase "access to." As revised, the regulations are consistent with approaches taken in other jurisdictions, such as GDPR and Colorado, while furthering the purposes of the CCPA and providing clarity to businesses about what decisions are in scope. This balances protections for consumer privacy and simplifying implementation for businesses at this time.
Costs	1471	Comment claims that the cybersecurity benefits cited by the Agency are flawed and based on faulty assumptions, including a mathematical error that	The Agency disagrees with this comment. The Agency made a good faith effort to estimate the costs associated with these regulations given available data and knowledge. The Agency acknowledges the arithmetic error, but notes that benefits actually increase when

		grossly inflates baseline cybercrime losses, and optimistic claims about risk reduction unsupported by empirical literature. The SRIA also fails to evaluate innovation incentives.	corrected. Also, respecting consumer privacy and data protection is not contrary to innovation and entrepreneurship; rather, the regulations foster the development of privacy-by-design products and services. The Agency has appropriately considered the impact on businesses and innovation. The regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Nevertheless, the Agency has modified the regulations to significantly reduce their costs
Costs	295, 434, 455	Comment states that the economic impact statement predicts a typical business will spend over $25,000 annually for a decade to comply, which imposes an undue and disproportionate financial burden on small businesses and startups. The regulations may lead to market pressures favoring larger firms and force smaller businesses and startups to forgo innovation and market opportunities. It will stifle growth and competition.	The Agency disagrees with this comment. Most of the costs of the regulations fall on larger businesses dealing with a large amount of personal information and with annual revenues that are greater than $28 million, not small businesses or startups. Moreover, respecting consumer privacy and data protection is not contrary to innovation and entrepreneurship; rather, the regulations foster the development of privacy-by-design products and services. Nevertheless, the Agency has modified the regulations to significantly reduce their costs, including for small businesses.
Costs	25, 34, 43, 52, 60, 71, 1656	Comment recommends phased implementations to ease the burden on businesses adapting to new standards.	The Agency agrees in part with this comment. The regulations have been revised to provide additional time for compliance with the ADMT and cybersecurity audit requirements to simplify implementation for businesses at this time. This includes a three-year phased implementation for cybersecurity audits. In addition, the submission requirements for both cybersecurity audit certifications and risk assessment information have been further simplified and the deadline to complete initial submissions has been extended to April 1, 2028.
Costs	26, 35, 44, 53, 61, 72	Comment suggests that the Agency should offer financial support or resources to help small businesses	The Agency disagrees in part with the comment. It is not within the Agency's mandate to provide financial support to small businesses to comply with the law. The Agency already provides, and will continue to provide, other non-monetary resources to small businesses (e.g., fact

		comply without experiencing undue strain.	sheets, advisories, online information) to help them understand the law and their obligations under it.
Costs	31, 39, 50, 57, 67	Comment is concerned that compliance documentation and regular audits consume valuable time and divert focus from core business activities.	The Agency disagrees with the intent of this comment. While the Agency acknowledges that documenting compliance and conducting regular audits will take time and resources, the regulations implement requirements mandated by the CCPA. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. They also generate significant benefits for businesses and consumers, such as reducing the risk of costly cybersecurity incidents.
Costs	119, 1945	Comment is concerned that the regulations would penalize growing businesses by imposing new burdens once they hit the 100,000 website-hits threshold.	The Agency disagrees with this comment. The 100,000 threshold is a requirement that comes from the definition of business in the CCPA. The regulations do not impose these supposed burdens, the statute does. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
Costs	126	Comment states that the regulations would create significant competitive disadvantages for businesses in California. It urges a revision of the rules to focus on privacy risks without overburdening the state's business community with excessive costs and complexities.	The Agency disagrees with this comment. The rules apply equally to all businesses handling large volumes of personal information that operate in CA, so there is no competitive advantage from being based outside CA. The instances where CA businesses are competing with other businesses in other state markets when the business competitors don't operate in CA are minimal, and as several other states pass and consider similar laws, CA businesses will be well positioned to adapt to other state rules. Moreover, the regulations will generate significant benefits for businesses and consumers, which over time, outweigh the direct costs associated with the regulations. Nevertheless, the Agency has modified the regulations to significantly reduce their costs.
Costs	1023	Comment argues that the reporting requirements in the regulations should undergo a more rigorous cost-benefit analysis to determine whether the costs of the regulations outweigh their	The Agency disagrees with this comment. The Agency made a good faith effort to estimate the costs associated with these regulations and has determined that the regulations will generate significant benefits for businesses and consumers, which over time, outweigh the direct costs associated with the regulations. Indeed, the cost-benefit

		purported benefits. The processing thresholds that trigger the requirements should also be increased to cover businesses that process (1) the personal information of 500,000 or more consumers or households, or (2) the sensitive personal information of 250,000 or more consumers.	analysis is rigorous and the benefits are likely underestimated because the calculation only accounts for a subset of pecuniary benefits and not all the benefits consumers will derive from the regulations. The CCPA requires businesses whose processing of consumers' personal information presents significant risk to consumers' security to perform an annual cybersecurity audit. The Agency has determined that processing the personal information of 250,000 or more consumers, or the sensitive personal information of 50,000 or more consumers, presents significant risk to consumers' security. The commenter has not provided any information as to why their proposed changes are more effective or appropriate than those adopted by the Agency. Nevertheless, the Agency has modified the regulations to simplify implementation for businesses at this time, which will also significantly reduce the costs of the regulations.
Costs	1103	Comment expresses concern that the cybersecurity regulations could raise homeownership costs by increasing costs for lenders and related industries.	The Agency disagrees with this comment. The regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Nevertheless, the Agency has modified the regulations to significantly reduce their costs. Direct costs over 10 years have decreased from $9.7 billion to $6.9 billion and overall quantifiable benefits have increased from $186 billion to $282 billion. The number of jobs lost in the first year also decreased and the number of jobs created over 10 years increased from 233,000 to 348,000. The gross state product in the 10th year also increased from $290 billion to $369 billion. Moreover, the Agency recognizes in the SRIA that not every cost can be estimated, which is why the Agency took a more general approach and focused on the areas that it expects to have the highest costs. Costs to consumers and the California economy at large are reflected in the Agency's macroeconomic impact estimates.
Costs	298, 563	Comment argues that compliance costs for required notices, access rights, opt-out facilitation, and data collection restrictions are prohibitively high for	The Agency disagrees with this comment. The majority of the costs of the regulations fall on larger businesses dealing with a large amount of personal information and with annual revenues that are greater than $28 million. Moreover, the CCPA directs the Agency to issue

		startups, especially those acting as service providers. The opt-out provisions, including those for ADMT, demand impractical operational changes, such as replacing automated processes with manual alternatives, which startups cannot afford.	regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The regulations balance providing privacy protections for consumers with flexibility for businesses to come into compliance. Nevertheless, the Agency has modified the regulations to significantly reduce their costs on small businesses. The range of first year costs for small businesses has decreased from $7,045 – $92,896 to $6,058 – $36,950.
Costs	300	The regulations will dissuade startups from offering and selling services to CA consumers and businesses. For example, an ADMT that uses data from a consumer-worn device to detect medical events and dispatch emergency aid if necessary couldn't function if a consumer opts out of ADMT. And because a company cannot "retaliate," i.e., not offer the service to consumers choosing to opt-out, the company would be forced not to offer the product in the first place. The regulations also produce knock-on impacts upon businesses, such as diminishing the ability of businesses to advertise to customers with whom they already have a relationship. They will reduce availability and increase prices for ADMT services, negatively impacting businesses that rely on these tools.	The Agency disagrees with this comment. Nevertheless, exercising its discretion, the Agency has modified the regulations to significantly reduce their costs, including on small businesses. For example, the Agency has revised the definition of ADMT to focus on the higher-risk use of ADMT, which is a use without any human involvement. Similarly, the Agency has revised the ADMT requirements to focus on the use of ADMT for significant decisions. The regulations also continue to include an exception for businesses using ADMT to ensure the physical safety of natural persons.
Costs	302	Comment states that the lack of adequate time for implementation of ADMT regulations creates undue	The Agency disagrees with this comment. However, the Agency has added § 7200(b) to provide a specific date, January 1, 2027, by which a business must comply with the ADMT requirements. This revision

		burden, especially for startups that lack the legal and technical resources to comply immediately. Startups need additional time and resources to meet the requirements while continuing critical business activities.	gives businesses additional time to implement the regulations. In addition, the Agency has revised § 7200 to focus on the use of ADMT for significant decisions, to simplify implementation at this time. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA.
Costs	471	Comment highlights the financial strain of compliance with the regulations. Comment also expresses concerns about additional indirect costs, such as lost sales due to poor customer experiences caused by intrusive pop-up notices and opt-out windows.	The Agency disagrees with this comment. The regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Nevertheless, the Agency has modified the regulations to significantly reduce their costs. Direct costs over 10 years have decreased from $9.7 billion to $6.9 billion and overall quantifiable benefits have increased from $186 billion to $282 billion. The number of jobs lost in the first year also decreased and the number of jobs created over 10 years increased from 233,000 to 348,000. The gross state product in the 10th year also increased from $290 billion to $369 billion. Also, regarding lost sales from pop-ups driving consumers away, the Agency recognizes in the SRIA that not every cost can be estimated, which is why the Agency took a more general approach and focused on the areas that it expects to have the highest costs. Costs to consumers and the California economy at large are reflected in the Agency's macroeconomic impact estimates. Furthermore, given privacy regulations already in existence, consumers are already faced with pop-ups when navigating to websites. Identifying the costs due to a possible additional pop-up is likely quite small.
Costs	1388	The SRIA underestimates the costs associated with the broad thresholds for cybersecurity audits, risk assessments, and ADMT obligations that are not targeted to activities likely to present a significant risk to consumers' privacy and security. For	The Agency disagrees with this comment. The Agency did consider these costs in its economic assessment, which captured a wide range of activities. Fiscal costs were also considered within the Economic and Fiscal Impact Statement. Regarding the impact of the regulations on businesses in other states without a physical presence in CA are outside the scope of the SRIA. Government Code § 11346.3(a) requires the SRIA to look at the regulation's impacts on California business

		example, the evaluation underestimates costs of building and maintaining ADMT access and opt-out rights, which could be significant given the scope of the activities that may be subject to these requirements. The SRIA also does not address the costs associated with reduction in revenue to the state and the cost of CPPA operations, which could meaningfully impact the projected operating deficit for the state.	enterprises. According to the California Employment Development Department methodology, this means firms with a physical presence in CA. The Agency has made a good faith effort to estimate the costs associated with these regulations on businesses with a physical presence in CA.
Costs	1390	The SRIA omits discussion of the year-over-year costs associated with the yearly audit and risk assessment requirements. A business subject to yearly reporting requirements will need to implement processes to track, document, and maintain compliance – a substantial feat for any business, especially small- and medium-sized businesses in the state.	The Agency disagrees with this comment. The comment is inaccurate. The SRIA looks at a decade of year-over-year costs associated with the cybersecurity audit, risk assessment, and ADMT regulations. Also, the yearly reporting requirement is required by the statute, not the regulations. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
Costs	1392	The SRIA should recognize the costs required to potentially hire independent auditors to conduct cybersecurity audits, including an accurate reflection of the cost for independent auditors that reflects the likely increase in demand for such services while the supply remains fixed (at least in the near term).	The Agency disagrees with this comment. The SRIA discusses the costs and reasonable estimates based on data regarding labor rates for independent auditors. The commenter has not provided any data to indicate an alternative labor rate is more accurate.
Costs	1393	The SRIA fails to acknowledge the impact and costs of the ADMT pre-use notice requirements, which are not	The Agency disagrees with this comment. The Agency made a good faith effort to estimate the costs associated with these regulations. The SRIA specifically notes that the hours required to update

		justified by the limited benefit to consumers who already receive multiple notices from businesses subject to the CCPA containing redundant information.	notification systems have been included in the overall hourly estimate. Nevertheless, the Agency has modified the ADMT regulations to focus on the use of ADMT for significant decisions, to simplify implementation at this time. The Agency has also revised the Pre-use Notice requirements, to provide businesses with flexibility in how they are consolidated or included with the Notice at Collection. The Pre-use Notice is not redundant, but rather ensures that consumers have meaningful information about the use of ADMT with respect to them when they exercise their CCPA rights.
Costs	1468, 1954, 1983	Comment highlights that the compliance costs are massive and the job loss projections are significant. Comment states that the SRIA underestimates total costs, including to the US economy at large. Comment argues that the SRIA does not include factors like external auditor and employee compensation rates, out-of-state businesses selling into California, productivity losses caused by compliance burdens, and key impacts on consumers.	The Agency disagrees with this comment. The Agency made a good faith effort to estimate the costs associated with these regulations given available data. Regarding labor costs, the SRIA discusses the costs and reasonable estimates based on data regarding labor rates for independent auditors and employees. The Agency did not include non-wage compensation because the Agency anticipates that the work would be done by existing salaried employees. Thus, the correct measurement is the number of hours it takes an employee to do a task. Regarding the impact of the regulations on businesses in other states without a physical presence in CA, they are outside the scope of the SRIA. Government Code § 11346.3(a) requires the SRIA to look at the regulation's impacts on California business enterprises. According to the California Employment Development Department methodology, this means firms with a physical presence in CA. The Agency has made a good faith effort to estimate the costs associated with these regulations on businesses with a physical presence in CA. Regarding other costs, the Agency recognizes in the SRIA that not every cost can be estimated, which is why the Agency took a more general approach and focused on the areas that it expects to have the highest costs. The Agency made a good faith effort to estimate the costs associated with these regulations given available data. Costs to consumers and the California economy at large are reflected in the Agency's macroeconomic impact estimates. Finally, the regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the

			regulations. Nevertheless, the Agency has modified the regulations to significantly reduce their costs.
Costs	1809	Comment critiques various benefit assumptions in the SRIA. Comment argues that increased transparency and consumer control is a direct benefit to consumers. However, benefits such as reduction in cybercrime or creation of new businesses are questionable.	The Agency disagrees in part with this comment. Both academic studies and private cybersecurity audit practitioners have provided supporting evidence for the effectiveness of the cybersecurity audit regulations in reducing potential monetary losses caused by cybercrimes. Increased security controls prevent data breaches from being as severe and as long, and can thwart some cybercrimes from occurring. The Agency also identified a number of non-quantifiable benefits from the regulations, which includes increased transparency and consumer control.
Costs	1810	Comment asserts that the Agency's analysis on financial impacts on consumers is missing. Consumers who exercise their privacy rights spend money and considerable amount of their time doing so.	The Agency disagrees with this comment. While there are some time costs associated with consumers exercising their rights, the purpose of the regulation is to make opt-out rights relatively seamless. Therefore, we believe these costs are overall a very small portion of total direct costs. Moreover, the vast majority of the cost associated with the exercising privacy rights are statutory and appropriately not included as a cost of these regulations.
Costs	2012	The regulations will cause CA to lose information jobs to other states where CA has no control over how that information will be regulated. CA will lose the jobs and the people who do those jobs to other states. This is similar to what happened with regard to California's environmental standards.	The Agency disagrees with this comment. While increased regulations could lead to decreased investment and jobs, the CA market is too significant for businesses that span state or country lines to ignore. It is not anticipated that those businesses will exit the California market entirely especially because many of these regulatory costs are coming or already exist in other jurisdictions. A global or US-wide company will have to meet similar regulatory requirements in other markets.
Costs	1948	New regulations often allow lawyers to prey on small businesses. Lawyers threaten to sue small businesses unless they pay a hefty settlement.	The Agency disagrees with this comment. The regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Moreover, most of the costs of the regulations fall on larger businesses dealing with a large amount of personal information and with annual revenues that are greater than $28 million. Also,

			there is no private right of action under the CCPA except with regard to data breaches. Nevertheless, the Agency has modified the regulations to significantly reduce their costs on small businesses. The range of first year costs for small businesses has decreased from $7,045 – $92,896 to $6,058 – $36,950.
Costs	518	Comment warns that having an over-inclusive definition of ADMT will require significantly more risk assessments. This will significantly increase costs for businesses of all sizes, will have downstream impacts on the services that consumers receive, and will increase administrative burden on the Agency.	The Agency disagrees with this comment. The regulations will generate significant benefits for businesses and consumers, which over time, greatly outweigh the direct costs associated with the regulations. Nevertheless, the Agency has modified the regulations, including the definition of ADMT, to significantly reduce the costs of the regulations. Direct costs over 10 years have decreased from $9.7 billion to $6.9 billion and overall quantifiable benefits have increased from $186 billion to $282 billion. The number of jobs lost in the first year also decreased and the number of jobs created over 10 years increased from 233,000 to 348,000. The gross state product in the 10th year also increased from $290 billion to $369 billion.

OTHER TOPICS – GENERAL

Section of Regulation	Comment Numbers	Summary of Comments 45-Day Comment Period	Agency Response
General	28, 46, 64, 326	Comment appreciates the Agency's role in empowering California residents with greater control over their personal data. Comment indicates that the Agency's efforts to refine regulations and strengthen consumer privacy protections are commendable.	The Agency agrees with this comment and notes commenter's support.
General	79, 109, 112, 115	Comment commends members of the Board, former Executive Director Soltani, and Agency staff for their commitment and dedication to giving guidance to California businesses, consumers, and workers on the most important and consequential data privacy policy in the United States.	The Agency agrees with this comment and notes commenter's support.

General	2042	Comment expresses gratitude to the Agency and its staff for their hard work enacting what was voted in by California voters, which created the Agency and the mandate for mandatory risk assessments and cybersecurity audits. The regulations are not overreach. It is the job of the Agency, and the Agency has no choice but to enact the regulations.	The Agency agrees with this comment and notes commenter's support.
General	1077, 1083	Comment appreciates the Agency's commitment to privacy rights and recognizes the significance of covering worker data in the CCPA regulations to ensure workers have control over their personal data. Comment appreciates the CPPA's leadership in data privacy and supports the inclusion of worker data in the CCPA regulations, positioning California as a national leader in protecting workers' rights in AI governance.	The Agency agrees with this comment and notes commenter's support.
General	1067	Comment commends the Agency for its dedication to guiding businesses, consumers, workers, and renters on critical data privacy policies. Comment supports the rulemaking, stating it will provide Californians with vital rights to transparency and recourse when AI and ADMT impact their lives.	The Agency agrees with this comment and notes commenter's support.
General	22, 32, 40, 68	Comment recognizes that the regulations are well intentioned.	The Agency agrees with this comment and notes commenter's support.
General	1106	Comment acknowledges the importance of regulations for emerging technologies and supports California's proactive stance. It agrees with several provisions of the regulations, including consolidating pre-use notice provisions, exemptions for security and fraud prevention use cases, and avoiding duplicative cybersecurity audits.	The Agency agrees with this comment and notes commenter's support.
General	1978	Comment indicates that it is critical for the Agency to enact policies that protect our communities as emerging	The Agency agrees with this comment and notes commenter's support.

		technologies intersect with the most consequential areas of the economy for everyday people where they live and the conditions under which they work. Public comments from industry represent some of the richest and most powerful companies in the world who are trying to block common sense frameworks to protect California's right to privacy, including how their personal information is collected, monitored, and decisions are made about them. The regulations strike a good balance between the desire to strengthen consumer privacy and the recognition of the importance of the information technology sector to the California economy.	
General	74	Comment urges the Agency to adopt the regulations to protect Californians' safety, privacy, and informed consent. These common-sense rules are crucial for consumer protection and human rights as algorithms increasingly impact housing, education, employment, and freedoms. The regulations should prioritize protecting people from discrimination and data exploitation rather than serving Big Tech's profits. Comment further encourages the Agency to stand firm in defending algorithmic transparency and accountability by adopting the regulations.	The Agency agrees with this comment and notes commenter's support for addressing consumer privacy harms across contexts.
General	89	Comment supports CCPA's overall structure and substance of the notice and access rights, and suggests that they should not be weakened in any future revisions of the regulations.	The Agency notes the commenter's support of the regulations. The Agency also notes the commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.
General	460	Comment expresses appreciation for the opportunity to provide input on these regulations, recognizing their significant impact on small businesses. Comment offers to work collaboratively with the Agency to address the	The Agency notes commenter's support and looks forward to continuing to work with stakeholders on future policy development.

		concerns outlined in their comments and ensure the regulations are fair and workable.	
General	962	Comment supports that the Agency has the legal authority to promulgate these regulations, as explicitly granted by the CCPA. Concerns about the Agency's jurisdiction are unfounded and should not distract from policy discussions. The Agency's mandate includes restricting or prohibiting processing if risks outweigh benefits.	The Agency agrees with this comment and notes commenter's support.
General	2045	Comment argues the Agency has the authority to regulate health care technologies through rulemaking to protect the data of health care workers and patients. California law guarantees workers a unique legal right to privacy in the workplace.	The Agency agrees with this comment and notes commenter's support.
General	503, 504	Comment believes the draft regulations exceed the scope of the CCPA, such as those that regulate back-end systems and publicly available information. For example, the ADMT regulations extend to back-end systems that do not interact with consumers.	The Agency disagrees with this comment. Comment does not explain how the Agency is regulating "back-end systems" and "publicly available information." With respect to back-end systems, they are subject to the regulations to the extent they are processing personal information and meet the relevant thresholds in a given section of the regulations. With respect to publicly available information, this is a defined term under the CCPA. The regulations do not, and cannot, amend the scope of the CCPA.
General	129, 322, 325, 330, 335, 462, 465, 468, 481, 514, 573, 652, 656, 768, 1122, 1127,	Comment argues that the Agency lacks the legislative authority to regulate, including with respect to AI, in such a broad manner. Comment contends that AI was not included in Proposition 24, the regulations are inconsistent with Governor's Newsom's executive order and recent veto of AI safety legislation, and the business community opposes the regulations. The Legislature recently passed, and Governor signed a number of laws	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purpose of the CCPA, as amended by the California Privacy Rights Act, which California voters overwhelmingly supported via passage of Proposition 24 in 2020. AB 1008's amendments to the CCPA support that the scope of "personal information" includes personal information

	1145, 1251, 1286, 1328, 1334, 1478, 1535, 1702, 1871, 1925, 1976, 1991, 2005, 2039	related to AI and none of them provided the CPPA with rulemaking authority. The Legislature also abandoned, or the Governor vetoed, a variety of ADMT proposals that the Agency now is attempting to enact through the regulations (e.g., requiring ADMT impact assessments, audits and testing, etc.). The Agency, led by five unelected board members, encroaches upon the role of the Legislature. ADMT requirements should be determined through the legislative process, allowing elected officials to weigh costs and benefits democratically. Comment suggests that the Agency abandon the regulations and allow Congress and the various state legislatures address this matter in due course. The Agency should focus on how existing access and opt-out rights apply to ADMT and on direct consumer privacy concerns. Also, the Agency's references to AB 1008 do not remedy the regulation's overreach. AB 1008 amendment to the definition of PI neither expands the scope of the statute to cover AI systems nor enlarges the agency's authority to create regulations touching on AI. The Legislature could have amended the grant of rulemaking authority to include AI systems, but did not do so. Also, AB 1008 was passed after the regulations were drafted. It cannot retroactively legitimatize the regulations. Comment asserts that the new rules impose unnecessary burdens and stray from the original voter-approved intent of limiting data sharing and allowing consumer data corrections. Comment asserts that since the proposed ADMT regulations include AI-related provisions, they violate Government Code § 11349(b), which requires a legal basis for regulatory actions. Additionally, the broad definition lumps different AI models and actors together, conflicting with other AI	that exists in AI systems. The regulations are not inconsistent with Governor Newsom's recent veto of SB 1047, which pertained to the safety and security of frontier AI models and did not focus on privacy. The Agency looks forward to continuing to work with stakeholders, including the Legislature and Governor Newsom, on future policy development. The CCPA directs the Agency to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' security to perform thorough and independent annual cybersecurity audits. The CCPA also directs the Agency to require businesses whose processing of consumers' personal information presents significant risk to consumers' privacy to conduct a risk assessment and submit it to the Agency on a regular basis. (Civ. Code § 1798.185(a)(14).) The CCPA further directs the Agency to issue regulations that govern access and opt-out rights with respect to businesses' use of ADMT. (*See* Civ. Code § 1798.185(a)(15).) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, it is required to issue regulations and impose certain requirements on these topics. Moreover, the Agency engaged in robust preliminary rulemaking activities with a wide variety of stakeholders, has collaborated with state lawmakers and will continue to do so. (*See* Civ. Code § 1798.199.40(g).) Nevertheless, exercising its discretion, the Agency has removed references to artificial intelligence as unnecessary. The CCPA and these regulations protect consumers' privacy and may apply to personal information processed by artificial intelligence whether stated expressly or not.

		frameworks. Comment argues that the CCPA is not an artificial intelligence law. The Agency is attempting to shoehorn artificial intelligence regulations into implementation of a privacy law. As a result, consumers would be inundated with frequent (if not constant) disclosure and opt-out notifications before interacting with AI-powered technologies, degrading their online experience and reducing overall engagement.	
General	262, 331, 396, 425, 478, 480, 519, 523, 1022, 1149, 1248, 1591, 2007, 2011	Comment contends that the regulations extend beyond what voters approved in Proposition 24, which focused on restricting data sharing and providing consumer protections. Comment claims the new requirements introduce additional compliance burdens that were not part of the measure's original scope and violate its requirement for regulatory balance between privacy protections and business impacts. Comment stresses the need for refinements to ensure legal alignment and feasibility. Comment suggests, to the extent possible, the Agency should tighten definitions so as not to impede beneficial and low-risk processing activities. Overly broad regulations can hinder businesses from prioritizing and focusing resources on privacy-enhancing measures that minimize risks, while forcing the Agency to devote resources to activities that do not present significant risks to consumer privacy and security. Commenter also asserts that the Agency does not have the resources, expertise, or skills at its disposal to implement these regulations effectively and to manage this very complicated important process, or to effectively review thousands of audits annually and determine if security measures align with appropriate risk profiles. Comment further asserts that attempting to rely on volunteers is an inadequate approach to regulating such	The Agency disagrees with this comment. Proposition 24 explicitly requires the Agency to issue regulations regarding cybersecurity audits, risk assessments, and ADMT, and as necessary to further the purpose of the CCPA, as amended by the California Privacy Rights Act, which California voters overwhelmingly supported via passage of Proposition 24 in 2020. However, using its discretion, the regulations have been revised to further simplify implementation and reduce costs for businesses at this time. The Agency also made revisions to provide further clarity to businesses; further, the regulations are also clear about their scope and relevant obligations for businesses. Additionally, the CPPA's staffing and resources take into account the CCPA requirement for the Agency to issue and determine compliance with these regulations. The Agency has not relied, nor is it attempting or planning to rely, on volunteers to regulate the industry. Further, the regulations require each business to submit a certificate of completion, not the full audit, annually. (*See* § 7124.)

		an important industry. Comment also asserts the regulations are vague.	
General	125, 207, 1176, 1180, 1181, 1843, 1956, 2030	Comment argues that Proposition 24 intended to establish the Agency as a consumer privacy watchdog. Comment states that the regulations go beyond the Agency's privacy-focused mission by regulating routine business tools and operations, as well as industries outside its jurisdiction. Comment further asserts that the regulations seek to control business decision-making in areas such as lending, housing, education, employment, and healthcare — areas beyond the agency's privacy mandate. Comment argues that the regulations should remain narrowly focused on consumer privacy risks and not extend into other areas. Comment argues that the regulations apply too broadly across industries without considering their varied impacts and should focus on key sectors such as employment, health, and housing instead of imposing uniform regulations. Comment supports that approach. The broad application of these new rules could create an uneven regulatory landscape that penalizes businesses for common practices and impedes innovation and day-to-day operations, while misallocating the Agency's resources to oversee matters that should fall under other regulatory bodies expertise. The Agency should scale back the regulations to what is clearly outlined in Proposition 24 by voters in 2020. Because the regulations turn on the broad category a business decision falls into, not the degree to which (or even whether) the decision implicates privacy, they are inconsistent with the privacy rationale explicitly stated in Prop. 24 and approved by the voters. And when coupled with the overly broad definition of ADMT, these regulations cover an astoundingly large swath of the economy that Prop. 24 could not have plausibly meant to	The Agency disagrees with this comment. Consumer privacy extends to the areas cited by the commenter. The suggestion that consumers should not have privacy protections in these areas is inconsistent with both the CCPA's statutory text and purpose. The CCPA explicitly provides privacy protections to employees and independent contractors, and provides consumers with rights to access and opt-out of ADMT. More broadly, it is intended to ensure that consumers have meaningful transparency and control over their personal information, which extends to ADMT that processes their personal information to make significant decisions about them. The regulations provide necessary privacy protections for consumers to address various consumer privacy harms across contexts. They have also been revised, including revisions to the scope of Article 11 and the definition of ADMT, to further simplify implementation for businesses at this time.

		regulate. The proposed rules plainly exceed their authorization in the CCPA and must instead be revised to cover only decisions with a significant privacy impact.	
General	135, 136, 137, 139, 145, 149, 150, 151, 154, 155, 156, 174, 177, 632	Comment contends that the regulations take an unprecedented approach, disregarding established frameworks from entities such as NIST and ISO. Comment argues that the Agency lacks the legal authority to regulate cyber audits, risk assessments, and ADMT beyond its statutory grant and the regulations are preempted by federal law. Comment states that the CCPA does not contain self-executing statutory requirements for cybersecurity audits, risk assessments, or automated decision-making. Instead, it grants the Agency discretion to design rules that align with federal regulations and avoid disrupting the banking sector. Comment indicates that financial institutions are already regulated under federal laws, such as the GLBA and the FCRA, and that the regulations infringe on the oversight authority of federal banking regulators and their affiliates, like the Office of the Comptroller of the Currency (OCC). Additionally, commenter asserts that 7124 and 7157 require banks to provide compliance documentation to the state constitute unauthorized "visitorial" oversight. Comment also argues that regulations interfere with core banking functions, such as underwriting, fraud prevention, and compliance, and could conflict federal safety and soundness standards. The rules could hinder banks' ability to use automated tools effectively, potentially weakening financial security and increasing risks for consumers.	The Agency disagrees with this comment. The regulations are within the Agency's delegated authority under the CCPA, as amended by the California Privacy Rights Act, which California voters overwhelmingly supported via passage of Proposition 24 in 2020. (*See* Civ. Code § 1798.185(a)(14)-(15).) In addition, the regulations apply to personal information as defined under the CCPA, and do not impose requirements on information that is subject to an exemption under the CCPA, such as those for FCRA and GLBA. The CCPA makes clear that the obligations imposed on businesses by the CCPA do not restrict a business's ability to comply with federal law and do not apply if preempted by, or in conflict with, federal law. (*See* Civ. Code §§ 1798.145(a)(1)(A), 1798.196).) Moreover, the CCPA includes a data-level exemption for information subject to the Gramm-Leach-Bliley Act and implementing regulations, but the CCPA applies to "businesses" and does not exempt financial institutions. (*See* Civ. Code §§ 1798.140(d), 1798.145(e).) Although the Agency strives for alignment with other laws, the Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The Agency must comply with California law and use its discretion to adopt requirements appropriate to California. To the extent a business is using NIST or ISO frameworks, it can leverage existing compliance processes when conducting risk assessments and cybersecurity audits under the CCPA. Additionally, the proposed regulations provide flexibility for businesses.

			Businesses can leverage existing processes to comply with ADMT requirements, and the regulations have been revised to further simplify implementation for businesses at this time.
General	1497, 1743	Comment commends the Agency for undertaking rulemaking to address ADMT, risk assessments, and cybersecurity. Comment recognizes that the Agency has a strong legal foundation under the CCPA and CPRA to issue the regulations. Comment indicates that the Agency's authority is broad, not limited to specific areas listed in Civil Code § 1798.185, and includes furthering the overarching purpose of protecting consumers' privacy rights under the CPRA § 3(A). In addition, comment emphasizes that control over the use of personal information is a key part of California's privacy history. Thus, regulations targeting misuse of personal information through AI directly serve the intended purpose of privacy protections.	The Agency agrees with this comment and notes commenter's support.
General	134, 307, 308, 768, 802, 1076, 1255, 1979	Comment contends that the Agency exceeds its statutory authority in regulating general technologies like ADMT, advertising practices, how businesses design and operate AI systems, cybersecurity controls, and other data processing activities. Comment urges the Agency to exercise regulatory humility and avoid adopting burdensome or overly broad regulations. Comment asserts that the Agency should focus on specific consumer privacy harms rather than attempting to regulate broad technologies or issues outside its mandate; the CCPA and CPRA were meant to give individuals control over their data. Comment believes that AI should be seen as part of the solution to privacy concerns and that policymakers should prioritize fostering innovation while addressing targeted	The Agency disagrees with this comment. The regulations are within the Agency's delegation of authority under the CCPA. (*See* Civ. Code § 1798.185(a)(14)–(15).) With respect to commenter's point about focusing on privacy harms, the regulations explicitly address processing that presents significant risk to consumers' privacy or security, and provide rights to opt-out and access ADMT for significant decisions concerning consumers. The Agency has made efforts to limit the burden of the regulations while implementing the CCPA. The regulations balance providing privacy protections for consumers with flexibility for businesses to come into compliance. Respecting consumer privacy and data protection is not contrary

		challenges. This expansion of regulatory power should be determined by the Legislature or voters, not through rulemaking.	to innovation and entrepreneurship; rather, the regulations foster the development of privacy-by-design products and services
General	652, 1097, 1031,1127, 1339, 1475, 1831, 1837, 1980, 2003	Comment argues that the regulations exceed the CCPA's authority in areas like first-party advertising, behavioral advertising, and training data regulation, which were not intended by the original law and do not pose significant risk. Comment argues that CCPA does not authorize a new advertising opt-out. Comment also asserts that consumers expect and benefit from first-party data processing for personalized content and advertising, and expanding opt-out rights beyond cross-context advertising exceeds the CCPA's authority. Comment further indicates that training exceeds the scope of the CCPA because it does not make a decision about a particular consumer and there is insufficient evidence training prevents a significant risk to privacy.	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purpose of the CCPA, as amended by the California Privacy Rights Act, which California voters overwhelmingly supported via passage of Proposition 24 in 2020. (*See* Civ. Code § 1798.185(a)(14)-(15).) In addition, the regulations have been revised to remove profiling for behavioral advertising and training thresholds have been removed from Article 11, to simplify implementation for businesses at this time. The risk assessment regulations require a risk assessment for certain training uses of consumers' personal information, because the Agency has determined that these uses present significant risk to consumers' privacy.
General	366, 1119, 1122, 1282, 1283, 1669	Comment argues that the rules do not align with CPRA's exemptions and urges explicit acknowledgment of CPRA's existing exemptions. Comment urges the Agency to amend the regulations to explicitly acknowledge CPRA's existing exemptions and ensure that they fully integrate existing exemptions under the CCPA, including opt-out rights, ADMT access rights, ADMT training, and profiling activities. Comment further recommends that any final rule reflects a broad scope of the Civil Code § 1798.145 exemptions; specifically, with respect to agents and service providers and representations about CCPA compliance.	The Agency disagrees with the comment. The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. The statutory exemptions apply to the regulations.
General	1670, 1671	Comment recommends that any final rule reflects those entities covered under the 1798.145 (d) and (e), FCRA and GLBA exemptions, may include agents or service	The Agency disagrees with this comment. The CCPA includes data-level exemptions, including for (1) information subject to the Gramm-Leach-Bliley Act

		providers under agreement with the user or furnisher that assist with the delivery, maintenance, analysis, and storage of consumer report information provided to the user and/or furnished by the furnisher. Comment suggests that where a CRA, User, or Furnisher represents that it complies with the CCPA, including the 1798.145 exemptions, a counter party or consumer should be expected to be able to rely on such assertion. The presence of litigation or enforcement activity — for example, over a vendor's reporting or dispute processes under the FCRA or GLBA — should not limit the right of the vendor to represent its compliance with the 1798.145 exemptions, and its customers to rely on such representation.	and implementing regulations or the California Financial Information Privacy Act, (2) information governed by HIPAA, and (3) the processing of personal information by certain entities, as long as the activity is regulated by the FCRA, and the processing is as authorized by the FCRA. (*See* Civ. Code §§ 1798.145(c)(1), (d), (e), 1798.146(a)(1), (4), (5).) These are not entity-level exemptions. In addition, to the extent a business is engaging in processing that is subject to the risk assessment and ADMT requirements, it must comply with those requirements. If its agents, vendors, or service providers are subject to the requirements for service providers or contractors under the CCPA, those entities must comply with the CCPA as well. The regulations are clear about the scope of businesses', service providers', and contractors' obligations, and additional modifications are not necessary.
General	11, 19, 27, 36, 45, 54, 62, 73, 132, 229, 433, 495, 526, 538, 553, 559, 767, 770, 1044, 1211, 1289, 1866, 1958,	Comment recommends that the Agency coordinate regulatory efforts with Governor Newsom, Legislature, and businesses to create a balanced regulatory approach. Comment contends that the draft regulations contradict the spirit of Governor Newsom's veto of SB 1047, which would have applied to developers of large AI models. Rushing forward without proper industry input could lead to negative economic and social consequences, as seen in past regulatory failures in California. Comment stresses that the Agency should not act unilaterally but instead work alongside the Legislature and Governor to ensure regulations align with existing laws and avoid unintended consequences. Comment also asserts that collaboration between	The Agency agrees in part with this comment. The Agency agrees that collaboration with businesses, the Governor, the Legislature, and other stakeholders is essential to implementing the CCPA's regulatory framework. The Agency notes that it has engaged in robust preliminary and formal rulemaking activities with a variety of stakeholders for this regulatory package. However, the regulations are issued pursuant to the CCPA's delegation of authority to the Agency. The Agency does not agree that the regulations should be withdrawn or delayed. The CCPA directs the Agency to issue regulations regarding cybersecurity audits, risk assessments, and ADMT. (Civ. Code § 1798.185(a)(14)-(15).) The

	2013, 2025	regulators and business owners is essential to create policies that protect consumers while allowing businesses to succeed. Comment suggests that the Agency engage more closely with small businesses to ensure their voices are heard and their challenges addressed. Comment encourages the Agency to also engage with businesses, technologists and educators to provide scalable adaptive frameworks that address AI related concerns without stifling progress. Comment stresses that the tech community is diverse, with middle tech companies playing a crucial role in AI innovation, productivity, and market competition. Some commenters urge the Agency to withdraw the regulations and take a broader, more inclusive approach to rulemaking. Comment argues that the ADMT regulations contradict Governor Newsom's call for AI governance led by experts in the field. Newsom's framework does not include the CCPA or the Agency for AI regulation.	Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA; thus, it is required to issue regulations and impose certain requirements on these topics. Moreover, the regulations are consistent with California law. The regulations are meant to be robust and applicable to many factual situations and across industries. The regulations balance providing protections for consumers' privacy while providing flexibility to businesses to come into compliance. Nevertheless, the Agency revised the regulations to further simplify implementation for businesses at this time. The Agency modified the regulations to focus on a higher-risk use of ADMT at this time, which is a use without any human involvement for significant decisions. This balances protections for consumer privacy and simplifies implementation for businesses at this time. The Agency also removed references to artificial intelligence. The Agency looks forward to continuing to work with stakeholders, including the Legislature and Governor Newsom, on future policy development.
General	1250	Comment states that stakeholders feel that their concerns have been largely ignored despite repeated input at board meetings. The regulations have remained mostly unchanged, raising doubts about whether the formal rulemaking process will address industry concerns. Despite concerns about the process and outcome, comment expresses a willingness to continue working with the Agency.	The Agency disagrees with this comment. The Agency engaged in robust preliminary and formal rulemaking activities with a wide variety of stakeholders, providing multiple and extensive opportunities for public comment. After reviewing and considering comments, including this comment, that were submitted during the initial comment period, the Agency revised the original proposed text of the regulations to simplify implementation and significantly reduced costs for businesses at this

			time. The Agency looks forward to continuing to work with stakeholders on future policy development.
General	304, 320, 323, 324, 437, 804	Comment suggests that the regulations should consider existing compliance efforts under other legal frameworks, such as those in different jurisdictions. Comment argues that AI is already well-regulated under existing sectoral laws like HIPAA, FCRA, and FERPA, as well as through consumer protection laws. Comment cautions against adding redundant regulations, advocating instead for addressing discrete gaps in existing laws. Comment highlights ongoing federal efforts to regulate AI, including bipartisan congressional studies, task force reports, and committee hearings. Comment also supports the Bipartisan House Task Force on AI's incremental approach to AI regulation, emphasizing regulatory restraint. Comment recommends that the regulations should be refined to prevent negative impacts on businesses while still protecting consumer privacy; comment suggest that leveraging existing regulatory frameworks and refining definitions would help balance privacy protections with industry needs. Clear articulation of how these regulations interact with existing laws will help businesses maintain consistent compliance. Comment also warns that California's broad AI regulations could lead to a fragmented regulatory environment across states, complicating compliance for businesses. Comment argues that AI regulation is an interstate commerce issue and should therefore be addressed at the federal level rather than through individual state laws.	The Agency agrees with this comment in part, to the extent it supports consideration of other legal frameworks. The Agency has considered other legal frameworks and the regulations are consistent with other jurisdictions when feasible. The Agency disagrees with this comment, to the extent that it suggests the regulations are redundant, overly broad, or unnecessary. The regulations are within the Agency's authority and further the intent and purpose of the CCPA, as amended by the California Privacy Rights Act, which California voters overwhelmingly supported via passage of Proposition 24 in 2020. However, the Agency has removed references to AI to further simplify implementation at this time.
General	1370	Comment asserts that the regulations must promote interoperability with other privacy frameworks and well-established standards. Harmonization benefits	The Agency notes commenter's suggestion.

		consumers' privacy and security by helping consumers understand and exercise their privacy rights and fostering a consistent compliance environment.	
General	763, 1012	Comment calls for the development of a national data privacy framework to avoid the complications of differing state laws, arguing that a fragmented regulatory landscape increases costs and complexity for businesses. Comment recommends that members of Congress work with their colleagues to make federal privacy protections.	To the extent the comment suggests the development of a national data privacy framework, the comment is not on the proposed action, but the Agency notes commenter's suggestion and looks forward to working with stakeholders on future policy development. While not on the proposed action, the Agency agrees with this comment to the extent that it advocates for broader protections for privacy.
General	1658, 1662	Comment argues that the regulations would stifle long-appreciated and expected consumer benefits offered by publishers. Readers could lose access to services they expect and appreciate, including content personalization, subscription offers, and advertising tailored to their interests, which is informed by their activity on publishers' sites. Comment warns that the regulations, if adopted without changes, would jeopardize the availability and affordability of quality journalism. Comment asserts that this is not the intent of the CCPA and is inconsistent with the law, including FTC guidance and other state privacy law. Commenter believes that this is an overreach which poses risk to access to journalism without adding any meaningful consumer privacy benefits.	The Agency disagrees with this comment. The regulations are within the Agency's authority and further the intent and purpose of the CCPA. (*See* Civ. Code § 1798.185(a)(14)-(15).) In addition, the regulations have been revised to remove the profiling for behavioral advertising and training thresholds have been removed from Article 11, to simplify implementation for businesses at this time.
General	1065	Comment argues that new regulations may create opportunities for lawyers to target small businesses with lawsuits over alleged noncompliance, forcing settlements that are financially and emotionally draining.	The Agency notes commenter's concerns. However, the regulations provide clarity to businesses about their obligations under the CCPA, which should make compliance easier for businesses. Additionally, the CCPA currently only allows for a private right of action if specific information related to the consumer

			is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices. (*See* Civ. Code § 1798.150.) The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA.
General	1957, 2006	Comment questions the transparency and accountability in the rulemaking process as only 32% California residents are aware of the Agency's role. Comment asks the Agency to slow down moving into rulemaking and to reconsider, because the draft requires significant redrafting. Comment believes that input was not considered despite repeated efforts to participate, and the potential to devastate the economy. From the public's perspective, the risk assessment and cyber audits regulations were introduced in September and the ADMTs in December 2023. Amendments were made available to the public only once, in March 2024, with no substantive changes thereafter. That's an eight-month window before regulations advanced into rulemaking, an entire legislative calendar in itself.	The Agency disagrees with this comment. The Agency was established by the California voters through Proposition 24. The Agency has provided all required notices in the rulemaking process and engages in public awareness activities to further the Agency's mission. Comment provides no information as to the basis for the assertion that only 32% of California residents are aware of the Agency's role. The timeline complies with the rulemaking process under the California Administrative Procedure Act, which requires the Agency to complete the process within one year from the date of notice. In addition, the Agency engaged in robust preliminary and formal rulemaking activities with a wide variety of stakeholders, which included the solicitation and consideration of preliminary comments before initiating the formal rulemaking process. The Agency looks forward to continuing to work with stakeholders on future policy development.
General	810	Comment provides answers to the Agency's invitation for preliminary comments on cybersecurity audits, risk assessments, and automated decisionmaking. Comment cites to the unfair and deceptive practices law.	Comment appears to be responding to the Agency's pre-rulemaking invitation for written comment, and citing unfair and deceptive practices laws that exist. The Agency notes the laws cited by commenter. The regulations are consistent with these laws.
General	761, 762	Comment argues that the current draft of the CCPA prioritizes the interests of businesses and government	The Agency disagrees with this comment, to the extent that it suggests that the regulations do not

		entities over consumer privacy. Comment argues that the current draft conceptualizes people as consumers, and consumers as passive entities. This is problematic given that people use the internet for reasons other than commerce, and that we live in a democracy, and democracies rely on active participation. The Agency should take a human-centric approach, not a business-centric or government-centric approach. It must be written in plain language that's easy for people to understand so we can use it; it must not have any loopholes; and it must, above all, avoid negating itself.	protect consumers' privacy. The regulations are within the Agency's delegation of authority under the CCPA and further the intent and purposes of the CCPA. They also balance providing privacy protections for consumers with flexibility for businesses in meeting their compliance obligations. The CCPA and the regulations ensure that consumers receive disclosures about the processing of their personal information and their CCPA rights, such as via a Pre-use Notice. They also ensure that consumers can easily opt-out, such as via opt-out links. With respect to compensation, the CCPA explicitly addresses financial incentives in § 1798.125(b). The Agency cannot amend the CCPA or adopt regulations inconsistent with the CCPA. In addition, the regulations have been further revised to simplify implementation for businesses at this time.
General	1066	Comment strongly supports maximum controls on AI and all social media platforms.	The Agency agrees with the comment, to the extent it supports the privacy protections in the regulations.
General	5, 6, 9, 10, 12, 13, 14, 15, 18, 220, 1062,	Comment relates to the Delete Act and data brokers. Comment recommends the accessible delete mechanism (DROP), which is being developed pursuant to the Delete Act, as a good initiative. Comment raises concerns related to the definition of "data broker" and "direct relationship," the annual fees, the impact on small businesses, that the technology is already existent in the private market, Comment encourages the Agency to prioritize increasing the number of data brokers registered in the system, rather than perfecting the DROP system. This will assist consumers with increased information of who holds their data and help then better use opt-out options through the DROP. Commenter	Comment relates to the Delete Act, a separate statute that regulates data brokers, which is implemented by the Agency and not the subject of the rulemaking. The proposed action only includes regulations implementing the CCPA. While not on the proposed action, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development. The Agency encourages commenters to participate in the Agency's rulemaking process for regulations implementing the Delete Act.

		requests clarity on determining a "match" under the Delete Act.	
General	1801, 1802	Comment advocates for full transparency on who consumers' information is shared with and why, especially before opting in to data sales. Comment states that one of the regulations currently in effect requires every business covered by the CCPA to have written contracts with service providers, contractors, and third parties that process consumers' personal information. However, consumers are not provided access to even minimal information like the date of the agreement.	While not on the proposed action, the Agency notes commenter's suggestion and looks forward to continuing to work with stakeholders on future policy development.

DRAFT