CALIFORNIA PRIVACY PROTECTION AGENCY
Board Meeting – December 8, 2023
Agenda Item 2

DESCRIPTION OF REVISIONS
PROPOSED RULEMAKING DRAFT: CYBERSECURITY AUDIT REGULATIONS

This chart provides a high-level summary of revisions to the draft text in "Proposed Rulemaking Draft: Cybersecurity Audit Regulations December 2023," specifically the items in single blue underline for additions and ~~single red strikethrough~~ for deletions. These are revisions relative to the "New Rules Subcommittee Revised Draft Cybersecurity Audit Regulations October 2023." Both documents are included with the meeting materials for Agenda Item 2 for the December 8, 2023 Board Meeting. Non-substantive changes (e.g., grammatical changes, changes in numbering/lettering, and corrections to section numbers) are not included.

SECTION	SUMMARY DESCRIPTION OF REVISIONS
7001	Deleted definitions of "cybersecurity incident" and "cybersecurity threat," because the draft no longer uses those terms in section 7023, subsection (b).
7001	Revised definition of "cybersecurity program" to replace "protect the security, confidentiality, integrity, and availability of personal information" with "protect personal information from unauthorized access, destruction, use, modification, or disclosure; and protect against unauthorized activity resulting in the loss of availability of personal information" to more specifically address the risks posed to consumers' security.
7001	Revised definition of "penetration testing" to add "by authorizing attempted penetration of the information system" for clarity.
7001	Revised definition of "privileged account" to delete "to make it more or less secure," because that language is unnecessary.
7050(g)	Revised "deems" to "requests as" to clarify that the relevant information that a service provider or contractor shall make available to the business's auditor is the information that the auditor requests, having deemed it necessary to complete the business's cybersecurity audit.
7120(b)	• (2): Selected the statutory threshold of Civil Code section 1798.140, subdivision (d)(1)(A), to align with the existing threshold in the statutory definition of "business." • (2)(A)–(C): Selected the three personal-information-processing thresholds that maximize protection for consumers' security, of those that had been included in "New Rules Subcommittee Revised Draft

SECTION	SUMMARY DESCRIPTION OF REVISIONS
	Cybersecurity Audit Regulations October 2023" for the December Board meeting (i.e., in the preceding calendar year, processed the personal information of 250,000+ consumers; processed the sensitive personal information of 50,000+ consumers; or processed the personal information of 50,000+ consumers the business had actual knowledge were <16 years of age).
7121(b), 7124(a)	Revised "annually" to "every calendar year" for clarity and consistency.
7122(a)(1)	Revised to streamline and clarify that an auditor shall not audit their own work, retaining examples of what an auditor shall not do.
7122(b)	Revised to clarify that the information the business shall make available to the business's auditor is the information that the auditor requests, having deemed it relevant to the business's cybersecurity audit.
7122(c)	Revised to add "make good-faith efforts."
7122(i), 7124(c)	Revised "authority to bind" to "authority to certify on behalf of" for clarity and consistency.
7123(a)	Revised and restructured to clarify and streamline the regulations: • Replaced the requirement that the audit assess and document "any risks from cybersecurity threats, including as a result of any cybersecurity incidents, that have materially affected or are reasonably likely to materially affect consumers" with "how the business's cybersecurity program protects personal information from unauthorized access, destruction, use, modification, or disclosure; and protects against unauthorized activity resulting in the loss of availability of personal information"; • Added option for the cybersecurity audit to assess and document how the business's cybersecurity program protects consumers from the negative impacts associated with unauthorized access, destruction, use, modification, or disclosure of personal information; and unauthorized activity resulting in the loss of availability of personal information, with high-level descriptions of the types of negative impacts; and • Moved requirement to assess and document the business's cybersecurity program to (b).

SECTION	SUMMARY DESCRIPTION OF REVISIONS
7123(b)(1), (c)(4)–(5)	Revised and restructured to clarify and streamline the regulations: • Moved requirement to include the responsible individuals and the date the cybersecurity program and evaluations thereof were presented to the board/governing body to (c)(4)–(5). • Deleted "the safeguards the business uses to protect personal information from internal and external risks to the security, confidentiality, integrity, or availability of personal information, including by protecting against the negative impacts set forth in subsections (b)(1)–(6)" as unnecessary, in light of the revised definition of "cybersecurity program" and the revisions to (b)(2), which continue to require the audit to assess and document each of the components of the business's cybersecurity program listed in (b)(2)(A)–(R), as applicable. • Added "identify" to (b)(1).
7123(b)(2), (f)	Replaced "safeguards" with "components" for consistency in referring to the list of "components" that the audit must assess and document.
7123(b)(2)(D)(iii)	Added "for employees, independent contractors, or other personnel; service providers or contractors; and privileged accounts" for clarity.
7123(b)(2)(F)(iii)	Revised "(e.g., systematically removing it or replacing it with asterisks)" to "(i.e., systematically removing or replacing with symbols such as asterisks or bullets)" and moved to directly after "masking" for clarity.
7123(b)(2)(M)(i)	Added "to whom the business provides access to its information system" for clarity.
7123(b)(2)(Q)(i)	Added definition of "security incident" for clarity and consistency.
7123(b)(4)	Added "Nothing in this section shall prohibit an audit from assessing and documenting components of a cybersecurity program that are not set forth in subsections (b)(1)–(2)" to provide flexibility for businesses and auditors.
7123(d), (e)	Added option for business to provide "a sample copy of the notification(s), excluding any personal information" to provide flexibility to businesses.
7123(e)	Replaced "a cybersecurity incident" with "unauthorized access, destruction, use, modification, or disclosure of personal information; or

SECTION	SUMMARY DESCRIPTION OF REVISIONS
	unauthorized activity resulting the loss of availability of personal information," because "cybersecurity incident" is no longer a defined term, and for clarity.
7123(f)	Added "or for another purpose" to account for that a business may have completed an audit not because it was required by another law or regulation but for another purpose.
7124(b)	Added "through the Agency's website" to indicate how businesses can submit their Notice of Compliance.