NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. The draft text in this document is intended to facilitate Board discussion and public participation and is subject to change.

PROPOSED RULEMAKING DRAFT: CYBERSECURITY AUDIT REGULATIONS

DECEMBER 2023

CPPA

NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. The draft text in this document is intended to facilitate Board discussion and public participation and is subject to change.

[ADDITIONS TO] § 7001. Definitions.

"Cybersecurity audit" means the annual cybersecurity audit that every business whose processing of consumers' personal information presents significant risk to consumers' security as set forth in section 7120, subsection (b), is required to complete.

"Cybersecurity program" means the policies, procedures, and practices that 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.

"Information system" means the resources (e.g., network, hardware, and software) organized for the processing of information, including the collection, use, disclosure, sale, sharing, and retention of personal information.

"Multi-factor authentication" means authentication through verification of at least two of the following types of authentication factors: (1) knowledge factors, such as a password; (2) possession factors, such as a token; or (3) inherence factors, such as a biometric characteristic.

"Penetration testing" means testing the security of an information system by attempting to circumvent or defeat its security features by authorizing attempted penetration of the information system.

"Privileged account" means any authorized user account (i.e., an account designed to be used by an individual) or service account (i.e., an account designed to be used only by a service, not by an individual) that can be used to perform functions that other user accounts are not authorized to perform, including but not limited to the ability to add, change, or remove other accounts, or make configuration changes to an information system.

"Zero trust architecture" means denying access to an information system and the information that it processes by default, and instead explicitly granting and enforcing only the minimal access required. Zero trust architecture is based upon the acknowledgment that threats exist both inside and outside of a business's information system, and it avoids granting access based upon any one attribute. For example, on an information system using zero trust architecture, neither the use of valid credentials nor presence on the network would, on its own, be sufficient to obtain access to information.

[ADDITION TO] § 7050. Service Providers and Contractors.

(g) A service provider or contractor shall, with respect to personal information that they collected pursuant to their written contract with the business, cooperate with the business in its completion of a cybersecurity audit pursuant to Article 9, including by making available to the business's auditor all relevant information that the auditor requests as necessary for the auditor to complete the business's cybersecurity audit; and not misrepresenting in any manner any fact that the auditor deems relevant to the business's cybersecurity audit.

NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. The draft text in this document is intended to facilitate Board discussion and public participation and is subject to change.

[MODIFICATION TO] § 7051. Contract Requirements for Service Providers and Contractors.
[Green double underline illustrates proposed additions to existing section 7051, subsection (a)(6).]

(a)(6) Require the service provider or contractor to comply with all applicable sections of the CCPA and these regulations, including—with respect to the personal information that it collected pursuant to the written contract with the business—providing the same level of privacy protection as required of businesses by the CCPA and these regulations. For example, the contract may require the service provider or contractor to cooperate with the business in responding to and complying with consumers' requests made pursuant to the CCPA, to assist the business in completing the business's cybersecurity audit pursuant to Article 9, to assist the business in conducting the business's risk assessment pursuant to Article 10, to assist the business in providing meaningful information to the consumer about its automated decisionmaking technology, and to implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Civil Code section 1798.81.5.

[ADDITION] ARTICLE 9. CYBERSECURITY AUDITS

§ 7120. Requirement to Complete a Cybersecurity Audit.

(a) Every business whose processing of consumers' personal information presents significant risk to consumers' security as set forth in subsection (b) shall complete a cybersecurity audit.

(b) A business's processing of consumers' personal information presents significant risk to consumers' security if any of the following is true:

(1) The business meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(C), in the preceding calendar year; or

(2) The business meets the threshold set forth in Civil Code section 1798.140, subdivision (d)(1)(A); and

(A) Processed the personal information of 250,000 or more consumers or households in the preceding calendar year; or

(B) Processed the sensitive personal information of 50,000 or more consumers in the preceding calendar year; or

(C) Processed the personal information of 50,000 or more consumers that the business had actual knowledge were less than 16 years of age in the preceding calendar year.

NOTE: The Agency has not yet started the formal rulemaking process for cybersecurity audits, risk assessments, or automated decisionmaking technology. The draft text in this document is intended to facilitate Board discussion and public participation and is subject to change.

§ 7121. Timing Requirements for Cybersecurity Audits.

(a) A business shall have 24 months from the effective date of these regulations to complete its first cybersecurity audit in compliance with the requirements in this Article.

(b) After the business completes its first cybersecurity audit pursuant to subsection (a), its subsequent cybersecurity audits shall be completed every calendar year, and there shall be no gap in the months covered by successive cybersecurity audits.

§ 7122. Thoroughness and Independence of Cybersecurity Audits.

(a) Every business required to complete a cybersecurity audit pursuant to this Article shall do so using a qualified, objective, independent professional ("auditor") using procedures and standards generally accepted in the profession of auditing.

(1) The auditor may be internal or external to the business but shall exercise objective and impartial judgment on all issues within the scope of the cybersecurity audit, shall be free to make decisions and assessments without influence by the business being audited, including the business's owners, managers, or employees; and shall not participate in activities that may compromise, or appear to compromise, the auditor's independence. For example, the auditor shall not participate in the business activities that the auditor may assess in the current or subsequent cybersecurity audits, including developing procedures, preparing the business's documents, or making recommendations regarding, implementing, or maintaining the business's cybersecurity program.

(2) If a business uses an internal auditor, the auditor shall report regarding cybersecurity audit issues directly to the business's board of directors or governing body, not to business management that has direct responsibility for the business's cybersecurity program. If no such board or equivalent body exists, the internal auditor shall report to the business's highest-ranking executive that does not have direct responsibility for the business's cybersecurity program. The business's board of directors, governing body, or highest-ranking executive that does not have direct responsibility for the business's cybersecurity program shall conduct the auditor's performance evaluation and determine the auditor's compensation.

(b) To enable the auditor to determine the scope of the cybersecurity audit and the criteria the cybersecurity audit will evaluate, the business shall make available to the auditor all information in the business's possession, custody, or control that the auditor requests as relevant to the cybersecurity audit (e.g., information about the business's

cybersecurity program and information system and the business's use of service providers or contractors).

(c) The business shall make good-faith efforts to disclose to the auditor all facts relevant to the cybersecurity audit and shall not misrepresent in any manner any fact relevant to the cybersecurity audit.

(d) The cybersecurity audit shall articulate its scope, articulate its criteria, and identify the specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) examined to make decisions and assessments, and explain why the scope of the cybersecurity audit, the criteria evaluated, and the evidence that the auditor examined is (1) appropriate for auditing the business's cybersecurity program, taking into account the business's size, complexity, and the nature and scope of its processing activities; and (2) why the specific evidence examined is sufficient to justify the auditor's findings. No finding of any cybersecurity audit shall rely primarily on assertions or attestations by the business's management. Cybersecurity audit findings shall rely primarily upon the specific evidence (including documents reviewed, sampling and testing performed, and interviews conducted) that is deemed appropriate by the auditor.

(e) The cybersecurity audit shall:

(1) Assess, document, and summarize each applicable component of the business's cybersecurity program set forth in section 7123;

(2) Specifically identify any gaps or weaknesses in the business's cybersecurity program;

(3) Specifically address the status of any gaps or weaknesses identified in any prior cybersecurity audit; and

(4) Specifically identify any corrections or amendments to any prior cybersecurity audits.

(f) The cybersecurity audit shall include the auditor's name, affiliation, and relevant qualifications.

(g) The cybersecurity audit shall include a statement that is signed and dated by each auditor that certifies that the auditor completed an independent review of the business's cybersecurity program and information system, exercised objective and impartial judgment on all issues within the scope of the cybersecurity audit, and did not rely primarily on assertions or attestations by the business's management.

(h) The cybersecurity audit shall be reported to the business's board of directors or governing body, or if no such board or equivalent body exists, to the highest-ranking executive in the business responsible for the business's cybersecurity program.

(i) The cybersecurity audit shall include a statement that is signed and dated by a member of the board or governing body, or if no such board or equivalent body exists, the business's highest-ranking executive with authority to certify on behalf of the business and who is responsible for the business's cybersecurity program. The statement shall include the signatory's name and title, and shall certify that the business has not influenced or made any attempt to influence the auditor's decisions or assessments regarding the cybersecurity audit. The statement also shall certify that the signatory has reviewed, and understands the findings of, the cybersecurity audit.

(j) The auditor shall retain all documents relevant to each cybersecurity audit for a minimum of five (5) years after completion of the cybersecurity audit.

§ 7123. Scope of Cybersecurity Audits.

(a) The cybersecurity audit shall assess and document 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. The cybersecurity audit also may assess and document how the businsess'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. Those negative impacts to consumers include impairing consumers' control over their personal information, as well as economic, physical, psychological, and reputational harm to consumers.

(b) The cybersecurity audit shall identify, assess, and document with specificity:

(1) The business's establishment, implementation, and maintenance of its cybersecurity program, including the related written documentation thereof (e.g., policies and procedures), that is 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, including the components set forth in this subsection and subsection (b)(2); and

(2) Each of the following components of the business's cybersecurity program, as applicable. If not applicable, the cybersecurity audit shall document and explain why the component is not necessary to the business's protection of personal information and how the safeguards that the business does have in place provide at least equivalent security:

(A) Authentication, including:

(i) Multi-factor authentication (including multi-factor authentication that is resistant to phishing attacks for employees, independent contractors, and any other personnel; service providers; and contractors); and

(ii) Strong unique passwords or passphrases (e.g., passwords that are at least eight characters in length, not on the business's disallowed list of commonly used passwords, and not reused).

(B) Encryption of personal information, at rest and in transit;

(C) Zero trust architecture (e.g., ensuring that connections within the business's information system are both encrypted and authenticated);

(D) Account management and access controls, including:

(i) Restricting each person's privileges and access to personal information to what is necessary for that person to perform their duties. For example:

(1) If the person is an employee, independent contractor, or any other personnel, restricting their privileges and access to personal information to what is necessary to perform the respective job functions of each individual, and revoking their privileges and access when their job functions no longer require them, including when their employment or contract is terminated;

(2) If the person is a service provider or contractor, restricting their privileges and access to personal information to what is necessary for the specific business purpose(s) set forth in, and in compliance with, the written contract between the business and the service provider or contractor required by the CCPA and section 7051; and

(3) Restricting the privileges and access of third parties to whom the business sells or shares personal information to the personal information that is necessary for the limited and specified purpose(s) set forth within the contract between the business and the third party required by the CCPA and section 7053;

(ii) Restricting the number of privileged accounts, restricting those privileged accounts' access functions to only those necessary to perform the account-holder's job, restricting the use of privileged accounts to when they are necessary to perform functions, and using a privileged-access management solution (e.g., to ensure just-in-time temporary assignment of privileged access);

(iii) Restricting and monitoring the creation of new accounts for employees, independent contractors, or other personnel; service providers or contractors; and privileged accounts, and ensuring that the accounts' access and privileges are limited as set forth in subsections (b)(2)(D)(i)–(ii); and

(iv) Restricting and monitoring physical access to personal information (e.g., through the use of badges, secure physical file locations, and enforcement of clean-desk policies).

(E) Inventory and management of personal information and the business's information system. This includes:

(i) Personal information inventories (e.g., maps and flows identifying where personal information is stored, and how it can be accessed) and the classification and tagging of personal information (e.g., how personal information is tagged and how those tags are used to control the use and disclosure of personal information);

(ii) Hardware and software inventories, and the use of allowlisting (i.e., discrete lists of authorized hardware and software to control what is permitted to connect to and execute on the business's information system); and

(iii) Hardware and software approval processes, and preventing the connection of unauthorized hardware and devices to the business's information system.

(F) Secure configuration of hardware and software, including:

(i) Software updates and upgrades;

(ii) Securing on-premises and cloud-based environments;

(iii) Masking (i.e., systematically removing or replacing with symbols such as asterisks or bullets) the sensitive personal information set forth in Civil Code section 1798.145, subdivisions (ae)(1)(A) and

(B) and other personal information as appropriate by default in applications;

(iv) Security patch management (e.g., receiving systematic notifications of security-related software updates and upgrades; and identifying, deploying, and verifying their implementation); and

(v) Change management (i.e., processes and procedures to ensure that changes to information system(s) do not undermine existing safeguards).

(G) Internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting (e.g., bug bounty and ethical hacking programs);

(H) Audit-log management, including the centralized storage, retention, and monitoring of logs;

(I) Network monitoring and defenses, including the deployment of:

(i) Bot-detection and intrusion-detection and intrusion-prevention systems (e.g., to detect unsuccessful login attempts, monitor the activity of authorized users; and detect unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information); and

(ii) Data-loss-prevention systems (e.g., software to detect and prevent unauthorized access, use, or disclosure of personal information).

(J) Antivirus and antimalware protections;

(K) Segmentation of an information system (e.g., via properly configured firewalls, routers, switches);

(L) Limitation and control of ports, services, and protocols;

(M) Cybersecurity awareness, education, and training, including:

(i) Training for each employee, independent contractor, and any other personnel to whom the business provides access to its information system (e.g., when their employment or contract begins, annually thereafter, and after a personal information security breach, as described in Civil Code section 1798.150); and

(ii) How the business maintains current knowledge of changing cybersecurity threats and countermeasures.

(N) Secure development and coding best practices, including code-reviews and testing;

(O) Oversight of service providers, contractors, and third parties to ensure compliance with sections 7051 and 7053;

(P) Retention schedules and proper disposal of personal information no longer required to be retained, by (1) shredding, (2) erasing, or (3) otherwise modifying the personal information in those records to make it unreadable or undecipherable through any means;

(Q) How the business manages its responses to security incidents (i.e., its incident response management);

(i) For the purposes of subsection (Q), "security incident" means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of the business's information system 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. Unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting the loss of availability of personal information is a security incident.

(ii) The business's incident response management includes:

(1) The business's documentation of predetermined instructions or procedures to detect, respond to, limit the consequences of, and recover from malicious attacks against its information system (i.e., the business's incident response plan); and

(2) How the business tests its incident-response capabilities; and

(R) Business-continuity and disaster-recovery plans, including data-recovery capabilities and backups.

(3) 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 shall describe, at a minimum, how the business implements and enforces compliance with them.

(4) 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).

(c) The cybersecurity audit shall:

(1) Assess and document the effectiveness of the components set forth in subsections (b)(1)–(2) in preventing unauthorized access, destruction, use, modification, or disclosure of personal information; and preventing unauthorized activity resulting in the loss of availability of personal information;

(2) Identify and describe in detail the status of any gaps or weaknesses of the components set forth in subsections (b)(1)–(2);

(3) Document the business's plan to address the gaps and weaknesses identified and described pursuant to subsection (c)(2), including the resources it has allocated to resolve them and the timeframe in which it will resolve them;

(4) Include the title(s) of the qualified individuals responsible for the business's cybersecurity program; and

(5) Include the date that the cybersecurity program and any evaluations thereof were presented to the business's board of directors or governing body or, if no such board or equivalent governing body exists, to the highest-ranking executive of the business responsible for the business's cybersecurity program;

(d) If the business provided notification to affected consumer(s) pursuant to Civil Code section 1798.82, subdivision (a), the cybersecurity audit shall include a sample copy of the notification(s), excluding any personal information; or a description of the notification(s).

(e) If the business was required to notify any agency with jurisdiction over privacy laws or other data processing authority in California, other states, territories, or countries of unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting the loss of availability of personal information, the cybersecurity audit shall include a sample copy of the notification(s), excluding any personal information; or a description of the required notification(s) as well as the date(s) and details of the activity that gave rise to the required notification(s) and any related remediation measures taken by the business.

(f) If the business has engaged in a cybersecurity audit, assessment, or evaluation that meets all of the requirements of this Article, the business is not required to complete a duplicative cybersecurity audit. However, the business shall specifically explain how the cybersecurity audit, assessment, or evaluation that it has completed meets all of the requirements set forth in this Article. The business shall address subsections (a)–(e) with

specificity, including explaining how the cybersecurity audit, assessment, or evaluation addresses each component set forth in subsections (b)(1)–(2). If the cybersecurity audit, assessment, or evaluation completed for the purpose of compliance with another law or regulation or for another purpose does not meet all of the requirements of this Article, the business shall supplement the cybersecurity audit with any additional information required to meet all of the requirements of this Article.

§ 7124. Notice of Compliance.

(a) Each business that is required to complete a cybersecurity audit pursuant to this Article shall submit to the Agency every calendar year either:

(1) A written certification that the business complied with the requirements set forth in this Article; or

(2) A written acknowledgment that the business did not fully comply with the requirements set forth in this Article. The written acknowledgement shall:

(A) Identify all sections and subsections of this Article that the business has not complied with and describe the nature and extent of such noncompliance; and

(B) Provide a remediation timeline or confirmation that remediation has been completed.

(b) The written certification or written acknowledgment shall be submitted to the Agency through the Agency's website and shall identify the 12 months that the audit covers.

(c) The written certification or written acknowledgment shall be signed and dated by a member of the board or governing body, or if no such board or equivalent body exists, the business's 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. It also shall include a statement that certifies that the signatory has reviewed and understands the findings of the cybersecurity audit. The signatory shall include their name and title.