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. Text preceded by "FOR BOARD DISCUSSION" presents topics for Board discussion.

NEW RULES SUBCOMMITTEE REVISED DRAFT RISK ASSESSMENT 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. Text preceded by "FOR BOARD DISCUSSION" presents topics for Board discussion.

Statutory Provisions for Reference:

Delegation of rulemaking authority to the California Privacy Protection Agency as set forth in Civil Code section 1798.185, subdivision (a)(15):

Issuing regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to:

(B) Submit to the California Privacy Protection Agency on a regular basis a risk assessment with respect to their processing of personal information, including whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public. Nothing in this section shall require a business to divulge trade secrets.

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. Text preceded by "FOR BOARD DISCUSSION" presents topics for Board discussion.

DRAFT RISK ASSESSMENTS REGULATIONS

[ADDITIONS TO] § 7001. Definitions.

"Artificial intelligence" means an engineered or machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs, such as predictions, recommendations, or decisions, that influence physical or virtual environments. Artificial intelligence includes generative models, such as large language models, that can learn from inputs and create new outputs, such as text, images, audio, or video; and facial- or speech-recognition or -detection technology.

"Automated decisionmaking technology" means any system, software, or process—including one derived from machine-learning, statistics, or other data-processing or artificial intelligence—that processes personal information and uses computation as whole or part of a system to make or execute a decision or facilitate human decisionmaking. Automated decisionmaking technology includes profiling.

"Decision that produces legal or similarly significant effects concerning a consumer" means a decision that results in access to, or the provision or denial of, financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment or independent contracting opportunities or compensation, healthcare services, or essential goods or services.

"Profiling" means any form of automated processing of personal information to evaluate certain personal aspects relating to a natural person and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

"Publicly accessible place" means a place that is open to or serves the public. Examples of publicly accessible places include shopping malls, stores, restaurants, cafes, movie theaters, amusement parks, convention centers, stadiums, gymnasiums, hospitals, medical clinics or offices, transportation depots, transit, streets, or parks.

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

(h) 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 conduct of a risk assessment pursuant to Article 10, including by making available to the business all facts necessary to conduct the risk assessment and not misrepresenting in any manner any fact necessary to conduct the risk assessment.

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. Text preceded by "FOR BOARD DISCUSSION" presents topics for Board discussion.

[MODIFICATIONS 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 10. RISK ASSESSMENTS

§ 7150. When a Business Shall Conduct a Risk Assessment.

(a) Every business whose processing of consumers' personal information presents significant risk to consumers' privacy as set forth in subsection (b) shall conduct a risk assessment before initiating that processing.

(b) Each of the following processing activities presents significant risk to consumers' privacy:

(1) Selling or sharing personal information.

(2) Processing sensitive personal information. However, a business that processes the sensitive personal information of its employees or independent contractors for the purposes of employment authorization, payroll, health-plan and benefits management, or wage reporting is not required to conduct a risk assessment for the processing of sensitive personal information for these purposes.

(3) Using automated decisionmaking technology in any of the following ways:

(A) For a decision that produces legal or similarly significant effects concerning a consumer;

(B) Profiling a consumer who is acting in their capacity as an employee, independent contractor, job applicant, or student. For example, this includes profiling an employee using keystroke loggers, productivity or attention monitors, video or audio recording or live-streaming, facial- or speech-recognition or -detection, automated emotion assessment, location trackers, speed trackers, and web-browsing, mobile-application, or social-media monitoring tools;

(C) Profiling a consumer while they are in a publicly accessible place. For example, this includes profiling a consumer while they are in a publicly accessible place using wi-fi or Bluetooth tracking, radio frequency identification, drones, video or audio recording or live-streaming, facial- or speech-recognition or -detection, automated emotion assessment, geofencing, location trackers, or license-plate recognition; or

(D) Profiling for behavioral advertising.

(4) Processing the personal information of consumers that the business has actual knowledge are less than 16 years of age.

(5) **FOR BOARD DISCUSSION:** Processing the personal information of consumers to train automated decisionmaking technology or artificial intelligence that may be used for any of the following:

(A) Any of the processing set forth in subsection (b)(3);

(B) Establishing individual identity on the basis of biometric information;

(C) Facial-, speech-, or emotion-detection;

(D) The generation of deep fakes (i.e., manipulated or synthetic audio, image, or video content that depicts a person saying or doing things they did not say or do and that are presented as truthful or authentic without the person's knowledge and permission); or

(E) The operation of generative models, such as large language models.

For purposes of this Article and the requirements for automated decisionmaking technology set forth in sections 7017, 7030, and 7031, "training" means teaching artificial intelligence or automated decisionmaking technology to generate a desired output. Training includes determining or improving the parameters of

the artificial intelligence or automated decisionmaking technology to achieve the desired output.

(c) Illustrative examples of when a business shall conduct a risk assessment:

(1) Business A is a rideshare provider. Business A seeks to use automated decisionmaking technology to allocate rides and determine fares and bonuses for its drivers. Business A shall conduct a risk assessment because it seeks to use automated decisionmaking technology for employment or independent contracting opportunities and compensation.

(2) Business B provides a mobile dating application. Business B seeks to disclose consumers' precise geolocation and the ethnicity and medical information the consumers provided in their dating profiles to Business B's analytics service provider. Business B shall conduct a risk assessment because it seeks to process sensitive personal information of consumers.

(3) Business C provides a personal-budgeting application into which consumers enter their financial information, including income. Business C seeks to display advertisements to these consumers on different websites for payday loans that are based on evaluations of these consumers' personal preferences, interests, and reliability. Business C shall conduct a risk assessment because it seeks to profile for behavioral advertising and share personal information.

(4) Business D provides delivery services. Business D seeks to install video cameras inside of its vehicles to observe its drivers' behavior and performance. Business D shall conduct a risk assessment because it seeks to profile its drivers.

(5) Business E is a grocery store chain. Business E seeks to process consumers' device media access control (MAC) addresses via wi-fi tracking to observe consumers' shopping patterns within its grocery stores. Business E shall conduct a risk assessment because it seeks to profile consumers in publicly accessible places.

(6) Business F is a technology provider. Business F seeks to process consumers' photographs and extract faceprints from them to train Business F's facial-recognition technology. Business F shall conduct a risk assessment because it seeks to process consumers' personal information to train automated decisionmaking technology or artificial intelligence that may be used for establishing individual identity on the basis of biometric information.

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. Text preceded by "FOR BOARD DISCUSSION" presents topics for Board discussion.

---

§ 7151. Stakeholder Involvement for Risk Assessments.

(a) A risk assessment shall involve all individuals from across the business's organizational structure who are responsible for preparing, contributing to, or reviewing the risk assessment. These individuals may include, for example, the business's product team, the business's fraud-prevention team, or the business's compliance team. These individuals shall disclose all facts necessary to conduct the risk assessment and shall not misrepresent in any manner any fact necessary to conduct the risk assessment.

(b) A risk assessment may rely on external parties to identify, assess, and mitigate the risks to consumers' privacy. These external parties may include, for example, service providers, contractors, providers of technological components as set forth in section 7153, subsection (a)(2)(C);[1] experts, including academics, who specialize in detecting and mitigating bias in automated decisionmaking technology; a subset of the consumers whose personal information the business seeks to process; or civil society organizations that represent consumers' or others' interests, including consumer advocacy organizations.

(1) For the uses of automated decisionmaking technology or artificial intelligence set forth in section 7150, subsections (b)(3) and (b)(5), if the business has not consulted external parties in its preparation or review of the risk assessment, the risk assessment shall include a plain language explanation addressing why the business did not do so and which safeguards it has implemented to address risks to consumers' privacy that may arise from the lack of external party consultation.

§ 7152. Risk Assessment Requirements.

(a) At a minimum, a risk assessment shall include the following information:

(1) **A short summary of the processing that presents significant risk to consumers' privacy.** The summary shall describe how the business will process the personal

[1] Section 7153, subsection (a)(2)(C) states: "If the business uses data, hardware, software, or other technological components provided by another person, including artificial intelligence or automated decisionmaking technology, the business shall provide the name(s) of the person(s), the name(s) of the technological component(s) provided, and how the business ensures that the technological component(s) provided do not negatively impact the validity, reliability, or fairness of the business's use of the automated decisionmaking technology (e.g., where the other person's reliability metrics differ from the business's)."

information, including how the business will collect, use, disclose, and retain personal information.

(A) For uses of automated decisionmaking technology as set forth in section 7150, subsection (b)(3), this summary also shall include an explanation of why the business is seeking to use the automated decisionmaking technology to achieve the purpose of the processing, including any benefits of using automated decisionmaking technology over the use of manual processing.

(2) **The categories of personal information** to be processed and whether they include sensitive personal information.

(A) For uses of automated decisionmaking technology or artificial intelligence as set forth in section 7150, subsections (b)(3) and (b)(5), the business also shall include the following:

(i) A plain language description of the personal information processed by the automated decisionmaking technology or artificial intelligence.

(ii) A plain language explanation of the steps the business has taken or any steps it plans to take to maintain the quality of personal information processed by the automated decisionmaking technology or artificial intelligence. "Quality of personal information" includes completeness, representativeness, timeliness, validity, accuracy, consistency; and reliability of the sources of the personal information (including the source from which the business obtained the personal information and, if known, the original source of the personal information) for the business's proposed use of the automated decisionmaking technology or artificial intelligence. For example, these steps may include removing incorrect or duplicative personal information or identifying personal information correlated with protected class(es) to mitigate the risk of discrimination.

(3) **The context of the processing activity,** including the relationship between the business and the consumers whose personal information will be processed.

(4) **The consumers' reasonable expectations concerning the purpose for processing their personal information, or the purpose's compatibility with the**

context in which their personal information was collected. The business shall describe consumers' reasonable expectations concerning the purpose for processing based on each factor identified in section 7002, subsection (b),[2] or the purpose's compatibility with the context in which the personal information was collected, based on the requirements identified in section 7002, subsection (c).[3] Alternatively, if the business plans to obtain consent for the processing, the business shall state so in the risk assessment and explain how the consent complies with section 7002, subsection (e).[4]

(5) **The operational elements of the processing.** At a minimum, the business shall describe the following:

(A) The business's planned method for collecting, using, disclosing, retaining, or otherwise processing personal information, including the sources of the personal information.

(B) How the business's processing of personal information complies with data minimization as set forth in section 7002, subsection (d)(1).[5] This explanation shall address why the business needs to process the personal

[2] Section 7002, subsection (b) states: "(1) The relationship between the consumer(s) and the business. . . . (2) The type, nature, and amount of personal information that the business seeks to collect or process. . . . (3) The source of the personal information and the business's method for collecting or processing it. . . . (4) The specificity, explicitness, prominence, and clarity of disclosures to the consumer(s) about the purpose for collecting or processing their personal information. . . . (5) The degree to which the involvement of service providers, contractors, third parties, or other entities in the collecting or processing of personal information is apparent to the consumer(s)."

[3] Section 7002, subsection (c) states: "(1) At the time of collection of the personal information, the reasonable expectations of the consumer(s) whose personal information is collected or processed concerning the purpose for which their personal information will be collected or processed. . . . (2) The other disclosed purpose for which the business seeks to further collect or process the consumer's personal information. . . . (3) The strength of the link between subsection (c)(1) and subsection (c)(2)."

[4] Section 7002, subsection (e) states: "A business shall obtain the consumer's consent in accordance with section 7004 before collecting or processing personal information for any purpose that does not meet the requirements set forth in subsection (a)."

[5] Section 7002, subsection (d)(1) states: "Whether a business's collection, use, retention, and/or sharing of a consumer's personal information is reasonably necessary and proportionate . . . shall be based on the following: (1) The minimum personal information that is necessary to achieve the purpose identified in compliance with subsection (a)(1) or (a)(2), or any purpose for which the business obtains consent. . . ."

information and the relevance of the personal information to the processing.

(C) How long the business will retain each category of personal information, and why the business needs to retain each category for that length of time. If the business has a retention policy or schedule that describes how long each category of personal information will be retained and why the business needs to retain each category for that length of time, the business may fulfill this requirement by appending, linking to, or otherwise incorporating such policy or schedule and making the retention policy or schedule available to the Agency as set forth in section 7158.

(D) The approximate number of consumers whose personal information the business plans to process.

(E) The technology to be used in the processing. For the uses of automated decisionmaking technology or artificial intelligence as set forth in section 7150, subsections (b)(3) and (b)(5), the business shall describe the appropriate purpose(s) for which it plans to use the automated decisionmaking technology or artificial intelligence and any limitations on its uses.

(F) The names of the service providers, contractors, or third parties to whom the business discloses or makes available the consumers' personal information for the processing, and the purpose for which the business discloses or makes the consumers' personal information available to them. If the business does not name each service provider, contractor, or third party, the business shall identify them by category. The business also shall explain with specificity why it did not name each service provider, contractor, or third party.

(G) For uses of automated decisionmaking technology as set forth in section 7150, subsection (b)(3), the assessment also shall include the output(s) of the automated decisionmaking technology, and how the business will use the output(s). For example, if the business seeks to use the automated decisionmaking technology to determine compensation for its employees or independent contractors, the business shall explain the outputs from the automated decisionmaking technology and how it uses these outputs to determine compensation.

(H) For uses of automated decisionmaking technology or artificial intelligence as set forth in section 7150, subsections (b)(3) and (b)(5), a plain language explanation of the logic of the automated decisionmaking technology or artificial intelligence, including any assumptions of the logic.

(6) **The purpose of processing consumers' personal information.** The business shall describe with specificity why the business needs to conduct the processing and how the processing achieves that purpose. The purpose shall not be described in generic terms, such as "to improve our services" or for "security purposes."

(7) **The benefits resulting from the processing to the business, the consumer, other stakeholders, and the public.** The business shall identify these benefits and describe them with specificity. For example, a business shall not identify a benefit as "improving our service," because this lacks specificity about what the specific improvements are to the service and how the benefit resulted from the processing. If the benefit resulting from the processing is that the business profits monetarily from the sale or sharing of consumers' personal information, the business shall state that this is the benefit and, when a business can estimate the expected profit, identify the estimated expected profit.

(8) **The negative impacts to consumers' privacy associated with the processing, including the sources of these negative impacts.** The business shall identify these negative impacts and the sources they stem from, and describe the magnitude of the negative impacts and likelihood of the negative impacts occurring. The business shall explain with specificity how it determined the magnitude and likelihood of the negative impacts, including the criteria the business used to make these determinations.

At a minimum, the business shall consider the following negative impacts to consumers' privacy as applicable to the processing activity:

(A) Constitutional harms, such as chilling or deterring consumers' free speech or expression, political participation, religious activity, free association, freedom of belief, freedom to explore ideas, or reproductive freedom; and harms to consumers' ability to engage in collective action or that impede the right to unionize.

(B) Cybersecurity harms as set forth in section 7123, subsection (b).

(C) Discrimination harms, including discrimination upon the basis of protected class(es) or their proxies, that has disparate impact upon

protected class(es), or that would violate federal or state antidiscrimination laws.

(D) Impairing consumers' control over their personal information, such as by providing insufficient information for consumers to make an informed decision regarding the processing of their personal information or by interfering with consumers' ability to make choices consistent with their reasonable expectations.

(E) Coercing or compelling consumers into allowing the processing of their personal information, such as by conditioning consumers' acquisition or use of an online service upon their disclosure of personal information that is unnecessary to the expected functionality of the service or requiring consumers to consent to processing when such consent cannot be freely given. For example, requiring an employee to consent to continuous video recording or otherwise be terminated presents a risk of coercing or compelling the employee into allowing the processing of their personal information, because the alternative of termination presents a risk that the employee's consent cannot be "freely given."

(F) Economic harms, including limiting or depriving consumers of economic opportunities; charging consumers higher prices; compensating consumers at lower rates; or imposing additional costs upon consumers, including costs associated with the unauthorized access to consumers' personal information.

(G) Physical harms, to consumers or to property, including processing that creates the opportunity for physical or sexual violence.

(H) Reputational harms, including stigmatization. Reputational harm includes stigmatization resulting from, for example, a mobile dating application's disclosure of a consumer's sexual or other preferences in a partner; a business stating or implying that a consumer has committed a crime without verifying this information; or a business processing consumers' biometric information to impersonate or mimic them via deepfake technology, generative artificial intelligence, or similar technology.

(I) Psychological harms, including emotional distress, stress, anxiety, embarrassment, fear, frustration, shame, and feelings of violation. Psychological harm includes, for example, emotional distress resulting from disclosure of nonconsensual intimate imagery; stress and

anxiety from regularly targeting a consumer who visits websites for substance abuse resources with advertisements for alcohol; or emotional distress from disclosing a consumer's purchase of pregnancy tests or emergency contraception for non-medical purposes.

(9) **The safeguards that the business plans to implement to address the negative impacts identified in subsection (a)(8).** The business shall explain how these safeguards address the negative impacts identified in subsection (a)(8) with specificity, including whether and how they eliminate or reduce the magnitude of the negative impacts or the likelihood of the negative impacts occurring; whether there are any residual risks remaining to consumers' privacy after these safeguards are implemented and what these residual risks are; and any safeguards the business will implement to maintain knowledge of emergent risks and countermeasures.

At a minimum, the business shall consider the implementation of the following safeguards as appropriate:

(A) Security controls such as encryption, data partitioning, physical and logical access controls, integrity monitoring, and data quality.

(B) Use of privacy-enhancing technologies such as trusted execution environments, federated learning, homomorphic encryption, and differential privacy.

(C) Restrictions on the collection and use of personal information as required under Civil Code 1798.100 (c)[6] and section 7002.

(D) Consulting the external parties such as those described in section 7151, subsection (b), at least every three years to ensure the business maintains current knowledge of emergent privacy risks and countermeasures, and using that knowledge to identify, assess, and mitigate risks to consumers' privacy.

[6] Civil Code 1798.100(c) states "A business' collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes."

(E) For processing as set forth in section 7150, subsection (b)(3), the requirements set forth in section 7153.

(10) **The business's assessment of whether the negative impacts identified in subsection (a)(8), as mitigated by the safeguards in subsection (a)(9), outweigh the benefits identified in subsection (a)(7).** The business shall describe with specificity how and why it determined that the negative impacts do or do not outweigh the benefits, including how any specific safeguards identified in subsection (a)(9) affect this assessment.

(11) **Relevant internal actors and external parties that have contributed to the risk assessment**. In the risk assessment or in a separate document maintained internally by the business, the business shall identify the internal actors and external parties that contributed to the risk assessment with sufficient information so that these actors or parties can be contacted, as necessary, to update the risk assessment and ensure its ongoing accuracy.

(12) **Any internal or external audit conducted that is relevant to the assessment,** including the name of the auditor, the names and positions of individuals involved in the review process, and the details of the audit process.

(13) **Dates the assessment was reviewed and approved, and names, positions, and signatures of the individuals responsible for the review and approval.** The individuals responsible for the review and approval shall include the individual who makes the determination about whether the business will initiate the processing that is subject to the risk assessment.

(14) **The date(s) that the risk assessment was presented or summarized to the business's board of directors or governing body**, or if no such board or equivalent body exists, the business's highest-ranking executive who is responsible for oversight of risk-assessment compliance.

§ 7153. Additional Requirements for Businesses Using Automated Decisionmaking Technology.

(a) If a business is using automated decisionmaking technology as set forth in section 7150, subsection (b)(3), the business's risk assessment also shall include the following:

(1) A plain language explanation of how the business evaluates its use of the automated decisionmaking technology for validity, reliability, and fairness. For purposes of this Article:

(A) "Validity" refers to confirmation that the automated decisionmaking technology, including its input(s), performs as intended for the business's proposed use(s), including the automated decisionmaking technology's accuracy in performing as intended.

(B) "Reliability" refers to the ability of the automated decisionmaking technology to perform as intended for the business's proposed use(s), repeatedly and without failure, under time interval(s) and conditions consistent with the business's proposed use(s).

(C) "Fairness" refers to equality, equity, and avoidance of discrimination harms.

(2) The plain language explanation required by subsection (a)(1) shall include:

(A) The metrics the business uses to measure validity, reliability, and fairness.

(B) Why the metrics selected in subsection (a)(2)(A) are appropriate measures of validity, reliability, and fairness.

(C) If the business uses data, hardware, software, or other technological components provided by another person, including artificial intelligence or automated decisionmaking technology, the business shall provide the name(s) of the person(s), the name(s) of the technological component(s) provided, and how the business ensures that the technological component(s) provided do not negatively impact the validity, reliability, or fairness of the business's use of the automated decisionmaking technology (e.g., where the other person's reliability metrics differ from the business's).

1. This explanation also shall include any copies of internal or external evaluations related to the technological component's validity, reliability, or fairness provided to or conducted by the business.

(D) Whether, and if so, how, the business evaluated other versions of the automated decisionmaking technology or other automated decisionmaking technologies for validity, reliability, or fairness for the business's proposed use(s).

(E) If the business evaluated other versions of the automated decisionmaking technology or other automated decisionmaking technologies for validity, reliability, or fairness for the business's proposed use(s), why the business seeks to use the version of the automated decisionmaking technology that it prefers to the other versions or other automated decisionmaking technologies.

(F) The results of the business's evaluations. For example, the business may provide an explanation of the performance and error metrics across demographic subgroups as part of the results of its fairness evaluation.

(3) The need for human involvement in the business's use of the automated decisionmaking technology. As part of this explanation, the business shall address the role and degree of any human involvement:

(A) Identify who at the business will be responsible for the business's use of the automated decisionmaking technology and for what they are responsible.

(B) Identify and describe the human's qualifications, if any, to understand the business's use of the automated decisionmaking technology, including the personal information processed by, and the logic and output(s) of, the automated decisionmaking technology.

(C) Explain whether and, if so, how the human evaluates the appropriateness of the personal information processed by, and the logic and output(s) of, the automated decisionmaking technology for the business's proposed use(s).

(D) Explain whether the human has the authority to influence whether or how the business uses the output(s) of the automated decisionmaking technology, and if so, how they exercise this authority.

(E) If the human can influence how the business uses the output(s) of the automated decisionmaking technology, explain whether and, if so, how the business uses the human's influence to calibrate the automated decisionmaking technology or the business's use of the automated decisionmaking technology.

(F) If a human is not involved in the business's use of the automated decisionmaking technology, explain why there is no human involvement, and which safeguards the business has implemented to address the risks to consumers' privacy that may arise from the lack of human involvement.

(b) For uses of automated decisionmaking technology as set forth in section 7150, subsection (b)(3), the risk assessment also shall explain how the business will provide a plain language explanation to a consumer in response to a request to access information about the business's use of automated decisionmaking technology, as set forth in section 7031.

§ 7154. Additional Disclosures for Businesses that Process Personal Information to Train Automated Decisionmaking Technology or Artificial Intelligence as Set Forth in Section 7150, Subsection (b)(5).

(a) If a business has processed or is processing personal information to train automated decisionmaking technology or artificial intelligence as set forth in section 7150, subsection (b)(5), and has made or is making that automated decisionmaking technology or artificial intelligence available to other persons for their own use, the business shall provide to those other persons a plain language explanation of the appropriate purposes for which the persons may use the automated decisionmaking technology or artificial intelligence and any limitations on these uses.

(1) The business shall document in its own risk assessment how it has provided or plans to provide the required information to those persons, and any safeguards the business has implemented or will implement to ensure that the automated decisionmaking technology or artificial intelligence is used for appropriate purposes by other persons.

(b) If a business has processed or is processing personal information to train automated decisionmaking technology or artificial intelligence, and has made or is making that automated decisionmaking technology or artificial intelligence available to other businesses ("recipient-businesses") for any processing activity set forth in section 7150, subsection (b), the business shall provide all facts necessary for those recipient-businesses to conduct the recipient-businesses' risk assessments.

(1) The business shall document in its own risk assessment how it has provided or plans to provide the necessary facts to those recipient-businesses.

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. Text preceded by "FOR BOARD DISCUSSION" presents topics for Board discussion.

---

§ 7155. Restriction on Processing If Risks to Consumers' Privacy Outweigh Benefits.

(a) The business shall not process personal information for any processing activity identified in section 7150, subsection (b), if the risks to consumers' privacy outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public.

§ 7156. Timing and Retention Requirements for Risk Assessments.

(a) A business shall comply with the following timing requirements for conducting and updating risk assessments:

(1) A business shall conduct and document a risk assessment in accordance with the requirements of this Article before initiating any processing activity identified in section 7150, subsection (b).

(2) At least once every three years, a business shall review, and update as necessary, its risk assessments to ensure that they remain accurate in accordance with the requirements of this Article.

(3) **FOR BOARD DISCUSSION:** At least [annually/once every two years/once every three years], a business shall review, and update as necessary, its risk assessments for uses of automated decisionmaking technology set forth in section 7150, subsection (b)(3).

(4) A business shall update a risk assessment whenever there is a material change relating to the processing activities. A change relating to the processing activities is material if it diminishes the benefits of the processing activities as referred to in section 7152, subsection (a)(7), creates new negative impacts or increases the magnitude or likelihood of already identified negative impacts referred to in section 7152, subsection (a)(8), or diminishes the effectiveness of the safeguards referred to in section 7152, subsection (a)(9).

Material changes may include changes to:

(A) The purpose of processing consumers' personal information.

(B) Consumers' reasonable expectations concerning the purpose for processing their personal information, or the purpose's compatibility with the context in which their personal information was collected. For example, if a business receives complaints from numerous consumers about risks to consumers' privacy caused by the processing, this may

indicate that consumers' reasonable expectations are not aligned with the business's processing.

(C) The minimum personal information that is necessary to achieve the purpose of the processing.

(D) The operational elements of the processing.

(b) Risk assessments, including prior versions that have been revised to account for a material change, shall be retained for as long as the processing continues, and for at least five years after the completion of the risk assessment or conclusion of the processing, whichever is later.

(c) 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 shall conduct and document a risk assessment in accordance with the requirements of this Article within [24 months] of the effective date of these regulations.

§ 7157. Conducting Risk Assessments for a Comparable Set of Processing Activities or in Compliance with Other Laws or Regulations.

(a) A business may conduct a single risk assessment for a comparable set of processing activities. A "comparable set of processing activities" that can be addressed by a single risk assessment is a set of similar processing activities that present similar risks to consumers' privacy.

(1) For example, Business G sells toys to children and is considering using in-store paper forms to collect names, mailing addresses, and birthdays from children that visit their stores, and to use that information to mail a coupon and list of age-appropriate toys to each child during the child's birth month and every November. Business G uses the same service providers and technology for each category of mailings across all stores. Business G shall conduct and document a risk assessment because it is processing personal information of consumers that it has actual knowledge are less than 16 years of age. Business G may use a single risk assessment for processing the personal information for the birthday mailing and November mailing across all stores because in each case it is collecting the same personal information in the same way for the purpose of sending coupons and age-appropriate toy lists to children, and this processing presents similar risks to consumers' privacy.

(b) If the business has conducted and documented a risk assessment for the purpose of complying with another law or regulation that meets all the requirements of this Article, the business is not required to conduct a duplicative risk assessment. [**FOR BOARD DISCUSSION:** A business [shall/may] specifically explain in an addendum to the risk assessment conducted and documented for compliance with another law how it meets all the requirements set forth in this Article.] If the risk assessment conducted and documented for the purpose of compliance with another law or regulation does not meet all the requirements of this Article, the business shall supplement the risk assessment with any additional information required to meet all of the requirements of this Article.

FOR BOARD DISCUSSION: § 7158. Submission of Risk Assessments to the Agency.

(a) **Annual Submission of Risk Assessment Materials.**

(1) **First Submission.** A business shall have [24 months] from the effective date of these regulations to submit the risk assessment materials regarding the risk assessments that it has conducted from the effective date of these regulations to the date of submission (hereinafter "first submission"). The risk assessment materials are set forth in subsection (b) and shall be submitted to the Agency as set forth in subsection (c).

(2) **Annual Submission.** After the business completes its first submission to the Agency as set forth in subsection (a)(1), its subsequent risk assessment materials shall be submitted every calendar year to the Agency, and there shall be no gap in the months covered by successive submissions of risk assessment materials (hereinafter "subsequent annual submissions").

(b) **Risk Assessment Materials to Be Submitted.** The first submission and subsequent annual submissions of the risk assessment materials to the Agency shall include the following:

(1) **Certification of Compliance.** The business shall submit a written certification that the business complied with the requirements set forth in this Article during the months covered by the first submission and subsequent annual submissions.

(A) The business shall designate a qualified individual with authority to certify compliance on behalf of the business. This individual shall be the business's highest-ranking executive who is responsible for oversight of

the business's risk-assessment compliance in accordance with this Article (hereinafter "designated executive").

(B) The written certification shall include:

(i) Identification of the months covered by the submission period for which the business is certifying compliance and the number of risk assessments that business conducted and documented during that submission period;

(ii) A statement that the designated executive has reviewed, understands, and approved the business's risk assessments that were conducted and documented in compliance with this Article;

(iii) A statement that the business initiated any of the processing set forth in section 7150, subsection (b), only after the business conducted and documented a risk assessment in compliance with this Article; and

(iv) The designated executive's name, title, and signature, and the date of certification.

(2) **Risk Assessments in Abridged Form:** A business shall submit its risk assessments in abridged form. For each risk assessment conducted and documented by the business during the submission period, the business shall submit an abridged version of the risk assessment that includes:

(A) Identification of the processing activities in section 7150, subsection (b), that triggered the risk assessment;

(B) The categories of personal information processed, including sensitive personal information, which shall be based upon section 7152, subsection (a)(2);

(C) A plain language explanation of the processing subject to the risk assessment, which shall be based upon section 7152, subsections (a)(1) and (a)(5);

(D) A plain language explanation of the purpose of the processing, which shall be based upon section 7152, subsection (a)(6); and

(E) A plain language explanation of why the negative impacts of the processing, as mitigated by safeguards, do or do not outweigh the benefits of the processing, which shall be based upon section 7152, subsection (a)(10).

(3) **Risk Assessments in Unabridged Form:** A business also may include in its submission to the Agency a hyperlink that, if clicked, will lead to a public webpage that contains its unabridged risk assessments.

(A) The business may redact trade secrets from an unabridged risk assessment, if the business provides an addendum that explains why the redacted material constitutes a trade secret.

(B) The business may redact the names and contact information of any individuals who contributed to, reviewed, or approved the risk assessment.

(C) The business may append, link to, or otherwise incorporate its retention policy or schedule for the processing subject to the risk assessment as set forth in section 7152, subsection (a)(5)(C).

(4) **Exemption.** A business is not required to submit a risk assessment to the Agency if the business does not initiate or otherwise engage in the processing subject to the risk assessment.

(c) **Method of Submission.** The risk assessment materials shall be submitted to the Agency using the Agency's risk assessment submission webpage.

(d) **Risk Assessments Shall Be Provided to the Agency Upon Request:** The Agency may require a business to provide its unabridged risk assessments to the Agency at any time. A business shall provide its unabridged risk assessments within five (5) business days of the Agency's request.