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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.**

DRAFT RISK ASSESSMENT REGULATIONS FOR CALIFORNIA PRIVACY PROTECTION AGENCY SEPTEMBER 8, 2023 BOARD MEETING

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. Underlined text is for additional Board consideration. Boxed text presents options 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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

DRAFT RISK ASSESSMENT REGULATIONS (EXCERPTS)

[ADDITIONS TO] § 7001. Definitions.

(c) "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.

(e) "Automated Decisionmaking Technology" means any system, software, or process—including one derived from machine-learning, statistics, other data-processing techniques, 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. "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.

[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.

[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

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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

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 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 furtherance of a decision that results in the provision or denial of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment or contracting opportunities or compensation, healthcare services, or access to essential goods, services, or opportunities.

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

(5) Processing the personal information of consumers who are employees, independent contractors, job applicants, or students using technology to monitor employees, independent contractors, job applicants, or students. Examples of such technology include 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 monitors.

(6) Processing the personal information of consumers in publicly accessible places using technology to monitor consumers' behavior, location, movements, or actions. Examples of such technology include 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.

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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

i. For purposes of this subsection, "publicly accessible places" means places that are open to or serve the public. Publicly accessible places include shopping malls, stores, restaurants, cafes, movie theaters, amusement parks, convention centers, stadiums, gymnasiums, hospitals, medical clinics or offices, transportation depots, privately-operated transit, streets, or parks.

(7) Processing the personal information of consumers to train artificial intelligence or Automated Decisionmaking Technology.

(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 Decision Technology in furtherance of 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 target these consumers with behavioral advertising on different websites for payday loans. Business C shall conduct a risk assessment because it seeks to 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 process drivers' personal information using technology to monitor employees or independent contractors.

(5) Business E is a grocery store chain. Business E seeks to process consumers' device 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 process the personal information of consumers in publicly accessible places using technology to monitor consumers' locations and movements.

(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 artificial intelligence.

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. Underlined text is for additional Board consideration. Boxed text presents options 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 involve 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)(5)(B)(3),[1] academics who specialize in detecting and mitigating bias in Automated Decisionmaking Technology, or a subset of the consumers whose personal information the business seeks to process.

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

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

(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

[1] Section 7153, subsection (a)(5)(B)(3), 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)."

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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

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 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

[2] Section 7002, subsection (b), states, "The consumer's (or consumers') reasonable expectations concerning the purpose for which their personal information will be collected or processed shall be based on the following: (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, "Whether another disclosed purpose is compatible with the context in which the personal information was collected shall be based on the following: (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. . . ."

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 ["Submission of Risk Assessments to the Agency"].

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

(E) The technology to be used in the processing.

(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 shall also explain with specificity why it did not name each service provider, contractor, or third party.

(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. [*Alternative Formulation*: The business shall identify these benefits and describe the magnitude of the beneficial impacts, and the likelihood of the beneficial impacts occurring. The business shall explain with specificity how it determined the magnitude and likelihood of the beneficial impacts, including the criteria the business used to make these determinations.]

(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:

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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

(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) Negative impacts to consumers' security as set forth in section 7123, subsection (b).[6]

(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.

(F) Exploiting consumers' vulnerabilities, such as age, employment or student status, immigration status, health status, or financial hardship. For example, a business that requires employees to consent to continuous video recording via their work computer or otherwise be terminated presents a risk of exploitation of their employment status because the employees cannot refuse without losing their employment.

(G) 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.

[6] Section 7123, subsection (b) includes an option that states: "[T]he following negative impacts to consumers' security: (1) Unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal information. . . ." and also identifies control, economic, physical, psychological, and reputational harms associated with the unauthorized access, destruction, use, modification, or disclosure of personal information; or unauthorized activity resulting in the loss of availability of personal 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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

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

(I) 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.

(J) 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 applicable to the processing activity:

(A) Safeguards to protect personal information such as encryption, segmentation, and access controls.

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

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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

(C) Restrictions on the processing of personal information as required under Civil Code section 1798.100, subdivision (c)[7] and section 7002.

(D) Deidentification or aggregation of personal information.

(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.

[7] Civil Code section 1798.100, subdivision (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."

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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

OPTIONS FOR BOARD CONSIDERATION FOR SECTION 7152, SUBSECTIONS (A)(11)–(13)/(14)

Option I for section 7152, subsections (a)(11)–(13):

(11) Relevant internal actors and external parties contributing to the assessment.

(12) Any internal or external audit conducted in relation 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.

Option II for section 7152, subsections (a)(11)–(14):

(11) The names and titles of the individuals within the business who prepared, contributed to, or reviewed the risk assessment, the individuals' qualifications, and the number of hours that these individuals worked on the risk assessment.

(12) The names or categories of external parties with whom the business consulted in preparing and reviewing the risk assessment, and the extent of these parties' involvement.

(13) The name and title of the highest-ranking executive with authority to bind the business and who is responsible for oversight of the business's risk-assessment compliance, and a statement that is signed and dated by the executive that certifies that the executive has reviewed, understands the contents of, and approved 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, if such board or equivalent body exists.

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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

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

(a) If a business is using Automated Decisionmaking Technology for the purposes set forth in sections 7030 and 7031 [processing that will be subject to Automated Decisionmaking Technology access/opt-out rights], the business's risk assessment shall also include the following:

(1) A plain language explanation of why the business is using or seeks to use the Automated Decisionmaking Technology to achieve the purpose of the processing, including any benefits of using the Technology over manual processing, the appropriate use(s) of the Automated Decisionmaking Technology, and any limitations on the appropriate use(s) of the Automated Decisionmaking Technology.

(2) A plain language explanation of the personal information processed by the Automated Decisionmaking Technology, including the personal information used to train the Technology and the sources of the personal information.

(3) A plain language explanation of the output(s) secured from the Automated Decisionmaking Technology and how the business will use the output(s). For example, if the business seeks to use Automated Decisionmaking Technology to determine compensation for its employees or contractors, the business shall explain the outputs from the Automated Decisionmaking Technology and how it uses these outputs to determine compensation.

(4) 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, including personal information used by the business to train the Technology. "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(s) of the Automated Decisionmaking Technology. 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.

(5) A plain language explanation of the logic of Automated Decisionmaking Technology, including any assumptions of the logic.

(6) A plain language explanation of the following:

(A) How the business evaluates its use of the Automated Decisionmaking Technology for validity, reliability, and fairness. For purposes of this Article:

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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

1. "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 Technology's accuracy in performing as intended.

2. "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).

3. "Fairness" refers to equality, equity, and avoidance of discrimination harms.

(B) The plain language explanation required by subsection (6)(A) shall include:

1. The metrics the business uses to measure validity, reliability, and fairness.

2. Why the metrics selected in subsection (6)(B)(1) are appropriate measures of validity, reliability, and fairness.

3. 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 identify 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).

    a. 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.

4. 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).

5. If the business evaluated other versions of the Automated Decisionmaking Technology or other Automated Decisionmaking

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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

Technologies for validity, reliability, or fairness for the business's proposed use(s), why the business did not use the other versions or Technologies.

6. 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.

(7) Supplementing the requirement under section 7152, subsection (a)(12), if the business has not consulted external parties in its preparation or review of the risk assessment, 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.

(8) A plain language explanation of the degree and details of any human involvement in the business's use of Automated Decisionmaking Technology. As part of this explanation, the business shall:

(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 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 Technology.

(F) If a human is not involved in the business's use of 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.

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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

(9) A plain language explanation of any safeguards that the business plans to implement to address the negative impacts to consumers' privacy that are specific to its use of Automated Decisionmaking Technology or for data sets produced by or derived from the Automated Decisionmaking Technology.

§ 7154. Additional Requirements for Businesses that Process Personal Information to Train Artificial Intelligence or Automated Decisionmaking Technology.

(a) If a business has processed or is processing personal information to train artificial intelligence or Automated Decisionmaking Technology, and has made or is making that artificial intelligence or Automated Decisionmaking Technology 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 artificial intelligence or Automated Decisionmaking Technology.

(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 artificial intelligence or Automated Decisionmaking Technology is used for appropriate purposes by other persons.

(b) If a business has processed or is processing personal information to train artificial intelligence or Automated Decisionmaking Technology, and has made or is making that artificial intelligence or Automated Decisionmaking Technology 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.

§ 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:

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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

(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).

OPTIONS FOR BOARD CONSIDERATION FOR SECTION 7156, SUBSECTION (A)(2)

Option I for section 7156, subsection (a)(2):

(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.

Option II for section 7156, subsection (a)(2):

(2) A business shall review, and update as necessary, its risk assessments to ensure they remain accurate in accordance with the requirements of this Article. Risk assessments for processing that uses Automated Decisionmaking Technology for the purposes set forth in sections 7030 and 7031 [processing that will be subject to Automated Decisionmaking Technology access/opt-out rights] shall be reviewed and updated at least [annually/biannually/once every three years].

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

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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

(D) The operational elements of the processing.

(E) The benefits resulting from the processing to the business, the consumer, other stakeholders, and the public.

(F) The negative impacts to consumers' privacy associated with the processing, including the sources of these negative impacts.

(G) The safeguards that the business has implemented or plans to implement to address the negative impacts identified in section 7152, subsection (a)(9).

(H) The business's assessment of whether the negative impacts identified in section 7152, subsection (a)(8), as mitigated by the safeguards in section 7152, subsection (a)(9), outweigh the benefits identified in section 7152, subsection (a)(7).

(I) Why the business is using or seeks to use Automated Decisionmaking Technology to achieve the purpose of the processing.

(J) The output(s) secured from the Automated Decisionmaking Technology and how the business will use the output(s).

(K) 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, including personal information used by the business to train the Technology.

(L) The logic of Automated Decisionmaking Technology and the assumptions of the Technology's logic.

(M) How the business evaluates its use of the Automated Decisionmaking Technology for validity, reliability, and fairness.

(N) The degree and details of any human involvement in the business's use of Automated Decisionmaking Technology.

(O) The safeguards that the business plans to implement to address the negative impacts to consumers' privacy that are specific to its use of Automated Decisionmaking Technology or for data sets produced by or derived from the Automated Decisionmaking Technology.

(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.

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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

(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. 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 of 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 of 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.

§ 7158. Submission of Risk Assessments to the Agency.

[**Summary of Requirements:** Businesses shall make risk assessments available to the Agency or the Attorney General upon request. Businesses also shall be required to annually submit to the Agency:

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. Underlined text is for additional Board consideration. Boxed text presents options for Board discussion.

(1) the business's risk assessments in an abridged form; and (2) a certification by a designated executive that the business has complied with the requirements in this Article.]