June 2, 2025

Business Software Alliance
Comments on Revised Proposed Regulations

The Business Software Alliance (BSA) appreciates the opportunity to comment on continued rulemaking by the California Privacy Protection Agency (CPPA). The agency's draft rules address critical topics, including automated decisionmaking technologies (ADMT), cybersecurity audits, and risk assessments. We appreciate many changes in the latest draft regulations but continue to believe further revisions are needed to create strong and workable privacy protections.

BSA is the leading advocate for the global software industry before governments and in the international marketplace.[1] Our members create the business-to-business technology products and services that power other companies. They offer tools including cloud storage services, customer relationship management software, cybersecurity solutions, human resources management programs, identity management services, and collaboration software. Businesses entrust some of their most sensitive information — including personal information — with BSA members. Our companies work hard to keep that trust. As a result, privacy and security are fundamental parts of BSA members' operations.

We appreciate recent changes to the proposed regulations but strongly encourage you to further revise all three sets of rules:

1. ***Automated Decisionmaking***. The recent revisions better focus the proposed ADMT regulations on ADMT technologies, rather than broader AI tools. However, the proposed regulations should be further revised to: (1) address practical concerns with treating allocation of work as a significant decision; (2) address issues with implementing pre-use notices, opt-outs, and access requests; and (3) harmonize them with other legislative and regulatory efforts.

2. ***Cybersecurity Audits***. Strong cybersecurity practices can help protect personal information but poorly targeted requirements will unduly burden companies without commensurate security benefits. We urge the CPPA to revise the proposed regulations on cybersecurity audits to: (1) expressly state that companies satisfy the CCPA's audit requirements if they conduct audits, certifications or evaluations under leading standards like ISO 27001 or SOC 2; (2) ensure any California-specific audit requirements are flexible, risk-based, and harmonized; and (3) limit audit requirements to personal information processed in a company's role as a business, not its role as a service provider.

3. ***Risk Assessments.*** Although BSA supports the use of risk assessments to identify and mitigate potential privacy risks, California will be an outlier in requiring businesses to proactively provide risk assessment information to the CPPA. We are concerned with this approach and strongly recommend: (1) promoting the use of global risk assessments, rather than California-specific requirements (2) removing requirements to provide information under penalty of perjury, (3) narrowing the set of information to be proactively provided to the CPPA, and (4) treating information provided to the CPPA as confidential.

[1] BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cohere, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

I. Automated Decisionmaking

BSA supports protecting consumers from high-risk uses of AI. For example, for several years we have called for legislation to ensure companies that develop and deploy AI for high-risk uses conduct impact assessments and adopt risk management programs.

We appreciate several revisions to the most recent proposed ADMT regulations and urge you to retain those changes. These include:

- Narrowing the definition of ADMT. We appreciate the new definition of ADMT as technology that either replaces or substantially replaces human decision-making. (Section 7001.) Narrowing this definition creates a more workable threshold for companies to implement the obligations created by the ADMT regulations, leading to greater certainty for both companies and consumers about which technologies are subject to heightened protections.

- Deleting the definition of Artificial Intelligence. The proposed regulations remove references to AI and instead focus on ADMT. We appreciate this approach, which decreases the potential for the ADMT rules to apply to broader AI systems in ways that are confusing and impractical. (Section 7001.)

- Narrowing the definition of significant decision. The proposed regulations narrow the types of decisions treated as "significant." We appreciate that the revised term focuses on decisions that result in the "provision or denial" of important benefits and services, rather than "access to" such services, which can inadvertently capture a wide range of non-significant actions. However, the list of significant decisions described in Section 7001(ddd)(1)-(6) should be further narrowed, as described below.

- Tailoring pre-use notices and consumer access requests to ADMTs used for significant decisions and protecting trade secrets. The proposed regulations narrow the requirements for pre-use notices and consumer access requests to ADMTs used for significant decisions, rather than broader uses of ADMTs. This change helps ensure that pre-use notices and consumer access requests apply to the uses of ADMT that have the most significant impact on consumers' daily lives. We strongly recommend keeping that focus and refining the obligations for pre-use notices and consumer access requests as described below. Additionally, the proposed regulations add new language to clarify that businesses providing pre-use notices or responding to access requests are not required to disclose trade secrets or information that may compromise their ability to protect against security threats and illegal activity. We strongly recommend keeping these provisions and strengthening them as described below. (Section 7220(d), Section 7222(c).)

- Focusing risk assessments on a more specific set of AI-related activities. The prior draft regulations would have required risk assessments for an extremely broad set of activities involving training either ADMT or AI. We strongly encourage you to retain the more focused approach in Section 7150(b)(6), which only requires risk assessments for companies training ADMT for significant decisions or specific sensitive activities.

We also urge you to make further changes to better focus the proposed ADMT regulations. Specifically, we encourage you to make three sets of changes:

First: Address practical concerns with treating allocation of work as a significant decision. The definition of significant decision includes employment or independent contracting opportunities or compensation — and identifies three types of opportunities, including allocation of assignment of work for employees. We are concerned that this part of the definition sweeps more broadly than intended. For example, an AI tool used to assign incoming calls at a call center should not be subject to the same requirements as a tool that accepts or rejects an applicant from the hiring process.

Recommendation:

- Section 7001(ddd) should be revised to clarify that significant decisions are those with material, legal, or similarly significant effects on a consumer. This would ensure that the protections focus on material risks to a consumer, without inadvertently sweeping in activities like work allocation, discussed above.
- The definition should add a provision stating: "An action is not a 'significant decision' if it does not have a material, legal, or similarly significant effect on a consumer."
- The definition of employment or independent contracting opportunities or compensation should be revised to strike allocation or assignment of work for employees.

Second: practical implementation challenges for pre-use notices, opt-outs, and access requests should be addressed.

The proposed regulations require businesses to comply with sweeping obligations before using ADMT for significant decisions. While we appreciate that requirements for pre-use notices, opt-outs of ADMT, and requests to access ADMT have been limited to ADMTs used for significant decisions, rather than applying to other uses of ADMT, these requirements present five concerns:

First, requirements for businesses to provide consumers with pre-use notices will likely result in over-notification to consumers. Pre-use notices to consumers must include at least seven specific explanations. That will result in lengthy notifications that consumers may be unlikely to read, undermining the protections created in the proposed regulations. We strongly recommend narrowing the information required in pre-use notices, so that notices are effective in alerting consumers about processing that may create concerns, not routine and expected processing.

Second, information to be provided for access requests creates practical concerns. The proposed regulations require businesses to disclose to consumers information in response to access requests, including information about the logic used in the ADMT and how the business used the output of the ADMT to make a significant decision about the consumer, the business's plans to use the outputs of the ADMT to make an additional significant decision concerning the consumer in the future, and the extent of human involvement in future significant decisions. Such sensitive details may include competitive or other confidential information. Although the proposed regulations include some protections for trade secrets, those provisions must be strengthened, as discussed below. Further, providing information about the logic behind individual consequential decisions may pose technical implementation challenges. Finally, we suggest removing requirements in to describe specific details of product improvements in response to access requests — both to avoid overly-long responses to consumers and to prevent disclosure of confidential information.

Third, protections for trade secrets should be expanded. While we appreciate that the proposed regulations provide new trade secrets protections for the pre-use notice and access rights, that language should be expanded. Specifically, it should protect "intellectual property or other confidential information," in addition to protecting trade secrets, to help ensure that companies can comply with the proposed regulations without putting at risk their business operations.

Fourth, the proposed regulations should clarify the scope of opt-outs to be implemented by service providers. The proposed regulations allow consumers to opt out of ADMTs used when a business makes a significant decision. However, in some circumstances the proposed regulations require a business to comply with a consumer's opt-out request by instructing all its service providers to remove a consumer from ADMT processing within a specified timeframe. This creates challenges because service providers do not generally have visibility into all the data they process on behalf of a business. Generally, service providers are subject to contractual and other protections that limit their access to personal data. The proposed regulations should be clarified to expressly state that service providers are only to implement opt-outs of the ADMT encompassed by the proposed regulations.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Fifth, exceptions to the opt out rights should be revised to make them workable in practice. The obligations for businesses to respond to consumers' opt out requests create several exceptions, including when ADMTs are used for admission, acceptance, or hiring decisions, and when ADMTs are used for allocation/assignment of work and compensation decisions. As a condition of both exceptions, the proposed regulations require that the ADMT works for the business's purpose and does not unlawfully discriminate based upon protected characteristics. That language in Section 7221 should be revised, because it is unclear how a company would determine that the ADMT "works" for its purposes. Instead, we recommend requiring a business to take reasonable steps to verify that the ADMT works for the business's purpose and to mitigate risks of unlawful discrimination based upon protected characteristics.

Recommendation: The CPPA should:

- Narrow the information required in pre-use notices.
- Ensure the information companies are required to provide in response to ADMT access requests is not unduly burdensome.
- Expand protections for trade secrets to also protect intellectual property and other confidential information.
- Clarify the scope of opt-outs to be implemented by service providers.
- Revise exceptions to opt-out rights in Section 7221 to focus on "taking reasonable steps" to ensure ADMT works for a business.

Third: The regulations should be harmonized with other legislative and regulatory efforts.

Today's technology ecosystem is global, and companies are developing strong compliance programs that can be leveraged across jurisdictions to support the responsible development and use of AI systems. As the CPPA addresses these issues, we strongly encourage you to account for the global context surrounding the draft regulations.

Even within California, legislators and other state regulators are advancing proposals to regulate the use of AI tools in circumstances likely to have the most significant impact on consumers' lives. BSA is concerned that efforts by the legislature, CPPA, and California Civil Rights Council (CCRC) risk imposing three different sets of rules on certain uses of automated tools — particularly in employment contexts — in just one state. Indeed, the broader context of AI regulation also counsels in favor of reading the CPPA's statutory authority to issue regulations on ADMT narrowly. Under the California Privacy Rights Act (CPRA), regulations are to govern "access and opt-out rights with respect to business's use of automated decisionmaking technology, including profiling." This authority is phrased narrowly, to focus on ADMT in the context of the access and opt-out rights already included in CPRA. The proposed regulations appear to go beyond this statutory mandate, in areas where other regulators and lawmakers are proposing and adopting policies.

Recommendation: The CPPA should work with its counterparts in the legislature and at the CCRC to help ensure consistency in proposed frameworks governing the use of automated tools. The CPPA should also read its statutory mandate to issue regulations on ADMT narrowly, to decrease opportunities for potential conflicts in regulatory frameworks.

II. Cybersecurity Audits

Data security is a critical aspect of protecting personal information. We appreciate several recent changes to the proposed regulations on cybersecurity, but strongly recommend the CPPA further leverage internationally-recognized audits and certifications — which in many cases, companies already conduct to demonstrate compliance with leading cybersecurity requirements.

Most importantly: the regulations should clearly treat companies as compliant with the CCPA's cybersecurity audit requirements if they conduct an audit or certification under

leading global cybersecurity standards, like ISO 27001 or SOC 2. Not only does this promote strong cybersecurity practices, it would also greatly reduce the economic impact of the proposed rules, which was a clear priority for several CPPA board members at the May 1 meeting.

We appreciate several revisions to the proposed cybersecurity regulations and urge you to retain those changes. These include:

- Involving a company's executive management team in audit oversight, rather than its board. The revised regulations require audits be reported to a business's executive management team, rather than its board. We strongly support this change, because board members are not themselves subject matter experts and should be able to rely on the expertise of cybersecurity and other personnel for information about cybersecurity risks.

- Referring to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The CSF sets the global standard for managing cybersecurity risks. We are pleased that the revised draft regulations refer to the CSF and strongly encourage you to further leverage this important tool to promote strong cybersecurity practices.

We also urge you to make three changes to improve the draft cybersecurity regulations.

First: The proposed regulations should expressly state that a company satisfies the CCPA's cybersecurity audit requirement if it conducts an audit, certification, or evaluation under leading standards, including ISO 27001 and SOC 2.

Companies already perform cybersecurity audits and assessments under globally-recognized standards and frameworks. The proposed regulations should recognize that these audits and certifications satisfy the CCPA. Not only would leveraging these existing cybersecurity audit tools promote leading cybersecurity practices, it would greatly reduce the economic impact of the regulations without compromising privacy or security. For example:

- In the United States, businesses conduct audits or assessments of their cybersecurity practices to comply with a range of federal laws including the *Sarbanes-Oxley Act (SOX)*, *Federal Acquisition Regulation (FAR*), and *Defense Federal Acquisition Regulations Supplement (DFARS)*. The United States Government also requires companies supplying products or services to federal agencies to comply with FedRAMP, the U.S. Department of Defense's Cybersecurity Maturity Model Certification (CMMC), and the Federal Information Processing Standards, among other requirements.

- Customers also frequently require their vendors to demonstrate strong cybersecurity practices — creating another layer of certifications and audit requirements that companies already do. For example, customers frequently require vendors to certify they are compliant with the ISO 27000-series of standards, which govern information security management.[2] Organizations perform internal audits of information security management systems to assess their compliance with the ISO 27001 standard and prepare for external audits, which are required to obtain ISO 27001 certification. This certification can only be issued by an accredited certification body. Likewise, under the American Institute of Certified Public Accountants' System and Organization Controls (SOC) framework, organizations obtain SOC 1, SOC 2, and/or SOC 3 reports and audits. The most comprehensive of these audits is SOC 2, which is an external audit performed by certified public accountants who must be independent of the organization they are assessing.

The CPPA should expressly recognize that existing audits and certifications satisfy the CCPA. The revised regulations take one step in this direction, by stating that a business may utilize a

[2] *See* ISO/IEC 27001 and related standards, *available at* https://www.iso.org/isoiec-27001-information-security.html.

cybersecurity audit, assessment, or evaluation that it has prepared for another purpose that meets the regulations' requirements — and specifically references the NIST CSF. But the regulations should go farther and list additional specific audits and certifications that satisfy the CCPA's requirements, to avoid imposing duplicative audit requirements without clear security benefits.

Instead of leveraging existing cybersecurity tools, the proposed regulations create California-specific audit requirements. This reinvents the wheel, creating additional and redundant audit obligations. Even worse, the California-specific requirements fail to clearly identify where they create obligations that are stricter than existing global frameworks. As a result, it is difficult for companies to map the existing cybersecurity audits they conduct against California's requirements. As the Regulatory Impact Assessment explains, four common security frameworks (the CSF, CIS Critical Security Controls v.8, ISO/IEC 27001, and SOC 2, Type II) each have "some overlap with the 18 core components" of California's proposed regulations.[3] But the proposed regulations do not clearly enable companies to leverage their use of well-established tools and audit frameworks.

The economic impact of this approach is significant. Companies that already conduct cybersecurity audits based on globally-recognized frameworks only reduce their cost of compliance with California's audit requirements by 30%, according to the Regulatory Impact Assessment. That means companies must pay for duplicative California-specific audits without a clear understanding of where the CPPA intends to create new requirements. This approach is also burdensome for the CPPA, because California-specific obligations will have to be updated over time by the agency. That duplicates work already done by other organizations, such as NIST updating its CSF or ISO updating the 27001 standards. We urge you to avoid this approach and instead treat companies as compliant with the CCPA if they already use leading existing audits, certifications, and frameworks.

Recommendation: Recognize that leading cybersecurity audits and certifications satisfy the CCPA. California-specific cybersecurity audits should only be contemplated if companies do not already conduct audits or certifications under existing frameworks. Specifically:

- Section 7123(f) should be modified to state: A business may utilize a cybersecurity audit, assessment, or evaluation that it has prepared for another purpose, provided that it is reasonably similar in scope to ~~meets all of the requiremetns of~~ this Article, either on its own or through supplementation. For example, a business may have engaged in an audit or certification that uses the National ~~i~~institute of Standards and Technology Cybersecurity Framework 2.0, ISO 27001 certifications, SOC 2 audits, FedRAMP authorization, or similar audits and certifications. Such audits and certifications ~~and~~ meet~~s all of~~ the requirements of this Article.

Second: Any California-specific audit requirements should be flexible, risk-based, and harmonized.

Companies should only be required to conduct California-specific cybersecurity audits if they do not already conduct the types of cybersecurity audits and certifications discussed above. Any California-specific requirements should be grounded in a flexible and risk-based approach, and promote consistency with existing standards, frameworks, and laws. This is especially important as cybersecurity regulations continue to increase internationally and at the federal and state level, each establishing new requirements and definitions that produce different approaches to compliance. CPPA should also issue guidance, such as crosswalks, that compare security controls under the

[3] *See* Standardized Regulatory Impact Assessment, Page 51 ("We assume that if a company utilizes an existing framework to assess its cybersecurity program, this will result in a 30% reduction in costs to complete the [cybersecurity audit]") (Nov. 22, 2024), *available at* https://cppa.ca.gov/regulations/pdf/ccpa_updates_cyber_risk_admt_ins_impact.pdf.

proposed regulations to common frameworks, standards, and auditing criteria such as the NIST CSF, ISO 27001, SOC 2, and programs like FedRAMP.

Recommendation: The CPPA should ensure that any California-specific requirements adopt a flexible, risk-based, and harmonized approach that is aligned to leading cybersecurity standards, frameworks, and laws. Such requirements should specifically leverage the NIST CSF, ISO 27001, and SOC 2. In addition, the CPPA should publish guidance including crosswalks between these California-specific requirements and leading frameworks, including the NIST CSF, ISO 27001, SOC 2, and programs like FedRAMP.

Third: The cybersecurity audit provisions should clearly focus on personal information a company processes in its role as a business and not as a service provider.

Businesses that process personal information in a manner that presents "significant risk" to consumers' security are required to complete cybersecurity audits under the draft regulations.

While this obligation is clearly placed on *businesses*, not service providers, the regulations are based on thresholds that may inadvertently wrap in personal information that a company processes in either its role as a business or its role as a service provider. Under the proposed regulations, processing presents a "significant risk" if a business processes a certain threshold of data. We are concerned that these thresholds do not account for the fact that some companies may process personal information as a business (for some products and services) and also process personal information as a service provider (for other products and services). Because the cybersecurity audit requirements apply to businesses — and not service providers — the proposed regulations should clearly state that the cybersecurity audit requirement and its thresholds only apply to personal information that companies process in their role as businesses.

Recommendation:

- Modify Section 7120(b) to state: A business's processing of consumers' personal information presents significant risk to consumers' security if any of the following is true for personal information it processes in its role as a business:
- Modify Section 7123(a) to state: The cybersecurity audit must assess how the business's cybersecurity program: protects personal information *that it processes in its role as a business* from unauthorized access, destruction, use, modification, or disclosure; and protects against unauthorized activity resulting in the loss of availability of personal information.

III. Risk Assessments

Data protection assessments are an important part of privacy compliance programs. BSA has supported a range of state and global privacy laws that require businesses to conduct data protection assessments of high-risk processing activities, which help companies identify and assess potential privacy risks and to adopt appropriate mitigation measures.

We appreciate several revisions to the most recent proposed regulations on risk assessments and urge you to retain those changes. These include:

- Narrowing the set of AI-related activities that will require risk assessments, by focusing on ADMT. The prior draft regulations would have required risk assessments of all processing used to train AI that is "capable of being used" for five broad activities. We appreciate the effort to more narrowly focus on processing that is intended to train an ADMT, identity verification, or physical or biological identification or profiling. (Section 7150(6).)

- Removing requirements to identify actions taken to maintain the quality of personal information processed by ADMT or AI. The prior draft regulations would have required risk

assessments to identify specific actions the business has taken to maintain quality of personal information, including a vague list of actions that do not easily apply across different types of AI-based processing. (Section 7152.)

- Focusing on information-sharing obligations for companies that make ADMT available to other businesses. The prior draft regulations would have required businesses that train both ADMT and AI and permit others to use it to provide a plain language explanation of limitations on the technology. We appreciate the current draft focuses instead on providing the recipient business with the facts available to the original business. (Section 7153.)

- Narrowing the set of materials to be provided to the CPPA. The prior draft regulations would have required businesses to submit abridged risk assessments to the CPPA, including the categories of personal information they process and the safeguards they implement. But that information is often confidential and disclosure creates trade secrets concerns. We appreciate the current draft narrowing the set of materials businesses must proactively provide to the agency — and recommend further narrowing them, as discussed below.

.

We also urge you to make five changes to the draft regulations on risk assessments.

First: Promote the use of risk assessments across jurisdictions.

Global companies have conducted privacy risk assessments for more than a decade. As a result, they have established processes for conducting and documenting such assessments, including under global privacy laws like the EU's General Data Protection Regulation (GDPR) and Brazil's General Data Protection Law (LGPD), and under state laws in 17 states.[4] We appreciate California's recognition that risk assessments are important — but the regulations should not adopt unique documentation requirements that fragment global compliance programs. Companies create stronger compliance programs that better protect consumers when they focus on developing a single set of risk management practices that apply across jurisdictions, instead of diverting resources to address a web of bespoke obligations.

The proposed regulations should promote the use of risk assessments across jurisdictions. The regulations start to acknowledge the importance of global risk assessments through Section 7156, which recognizes that when a business conducts a data protection assessment for the purpose of complying with another jurisdiction's law or regulations, it may also satisfy the obligations under CCPA. We strongly recommend that language go farther, to recognize that impact assessments satisfy the CCPA's obligations if they are reasonably similar in scope to the proposed regulations.

Recommendation:

- Modify Section 7156 to state: A business may utilize a risk assessment that it has prepared for another purpose to meet the requirements in section 7152, provided that the risk assessment is reasonably similar in scope ~~contains the information that must be included in, or is paired with the outstanding information necessary for, compliance~~ with section 7152.

Second: Do not require risk assessment information be submitted under penalty of perjury.

The proposed regulations require risk assessments be submitted to the agency under penalty of perjury. Specifically, the employee submitting risk assessment information to the CPPA must attest that: (1) the business has conducted a risk assessment, (2) that the employee meets the requirements imposed by the regulations to submit a risk assessment, and (3) that the information is true and correct. That submission is to be made under penalty of perjury.

[4] *See*: BSA's Models of State Privacy Legislation, *available at* https://www.bsa.org/policy-filings/us-2024-models-of-state-privacy-legislation.

In California, perjury is punishable by up to four years imprisonment.[5] Imposing criminal penalties under these circumstances is disproportionate to the harm the regulations seek to address, of ensuring that the CPPA is provided truthful information. We strongly urge you to remove any language requiring risk assessment information be provided under penalty of perjury.

Recommendation:

- Modify Section 7157(b)(5) to state: Attestation to the following statement: "I attest that the business has conducted a risk assessment for the processing activities set forth in California Code of Regulations, Title 11, section 7150, subsection (b), during the time period covered by this submission, and that I meet the requirements of section 7157, subsection (c). ~~Under penalty of perjury under the laws of the state of California,~~ I hereby declare that the risk assessment information submitted is true and correct."

Third: Narrow the set of activities requiring risk assessments.

The proposed regulations require risk assessments for six types of processing. We recommend revising two of the scenarios for which assessments are required:

- First, Section 7150(b)(1) should be narrowed to require a risk assessment when a business sells or shares *sensitive personal information*, rather than all personal information. This can help reduce uncertainty around tracking technologies like cookies, and whether they are deemed to "share" information. Requiring a risk assessment for use of any tracking cookies would significantly expand the requirement to conduct assessments, without clear benefits.

- Second, we recommend clarifying that the processing of sensitive personal information in employment-related contexts is exempt, by broadening Section 7150(b)(2)(A). The current language can be read narrowly, in ways that create different requirements for similar types of employment-related processing activities.

Recommendation:

- Modify Section 7150(b)(1) to state: selling or sharing sensitive personal information.
- Modify Section 7150(b)(2)(A) to state: A business that processes the sensitive personal information of its employees or independent contractors solely and specifically for employment-related purposes ~~of administering compensation payments, determining and storing employment authorization, administering employment benefits, providing reasonable accommodation as required by law, or wage reporting as required by law,~~ is not required to conduct a risk assessment for the processing of sensitive personal information for these purposes. Any other processing of consumers' sensitive personal information is subject to the risk-assessment requirements set forth in this Article.

Fourth: Clarify that risk assessment information does not include specific types of personal information.

The proposed regulations require businesses to proactively provide the CPPA with specific risk assessment information. This makes California an outlier, and we strongly recommend the regulations avoid requiring disclosure of detailed information about risk assessments. The current text could be read to require companies to disclose specific types of personal information they process, by requiring a business to state "whether the risk assessment . . . involved the processing of each of the categories of personal information and sensitive personal information" covered by the CCPA.

[5] Cal. Penal Code § 118.

We strongly encourage you to make clear that businesses only need to state in the risk assessment information whether they process either personal information or sensitive personal information, as those terms are defined in the CCPA. The regulations should not require businesses to list the specific types of personal information they process, which can create a range of privacy and security concerns. For example, if cybersecurity company discloses the categories of information it processes to detect threats, it can create a roadmap for bad actors to circumvent security protections. This concern is compounded because the proposed regulations do not appear to limit the CPPA's further disclosure or use of the risk assessment information.

Recommendation:

- Modify Section 7157(b)(4) to state: Whether the risk assessments conducted or updated by the business during the time period covered by the submission involved the processing of personal information or sensitive personal information, as those terms are defined ~~each of the categories of personal information identified~~ in Civil Code section 1798.140, subdivisions (v)(1)(A)-(L), (ae)(1)(A)-(G), and (ae)(2)(A)-(C).

Fifth: Treat risk assessment information provided to the CPPA as confidential.

The proposed regulations should also be revised to protect any risk assessment information disclosed to the agency. We strongly encourage you to revise the proposed rules to ensure: (1) risk assessment information provided to the CPPA is treated as confidential and exempt from disclosure under open records law, (2) disclosure of risk assessment information to the agency does not constitute a waiver of attorney-client privilege, work product protection, or other applicable protections.[6] This will not only help avoid inadvertent disclosure of proprietary data and business practices that may be reflected in a risk assessment, but also create strong incentives for companies to undertake rigorous risk assessments.

Recommendation:

- A new provision should state: Confidentiality. Risk assessment materials disclosed to the Agency are to be treated as confidential by default and are exempt from open records laws. In addition, providing materials to the Agency does not constitute a waiver of attorney-client privilege, work product protection, or other applicable protections.

* * *

BSA supports strong privacy protections for consumers, and we appreciate the opportunity to provide these comments. We welcome an opportunity to discuss these important issues.

For further information, please contact:

Meghan Pensyl
Director, Policy
meghanp@bsa.org

Kate Goodloe
Managing Director, Policy
kateg@bsa.org

Business Software Alliance

[6] This protection is provided by other state privacy laws. *See, e.g.*, Colo. Rev. Stat. § 6-1-1309(4); Conn. Gen. Stat. § 42-529b(f); 6 Del. C., § 12D-108(c); Fla. Stat. § 501.713(3); Ind. Code § 24-15-6-2(b); Ky. Rev. Stat. Ann. § 367.3621(4-5); Md. Code Ann., Com. Law, § 14–4710(d)(3); Minn. Stat. § 325O.08(f); Mont. Code Ann. § 30-14-2814(3)(c-d); Neb. Rev. Stat. § 87-1116(4); N.H. Rev. Stat. Ann. § 507-H:8(III); N.J. Rev. Stat. § 56:8-166.12(b); Or. Rev. Stat. § 646A.586(7); R.I. Gen. Laws § 6-48.1-7(f); Tenn. Code Ann. § 47-18-3307(c); Tex. Bus. & Com. Code Ann. § 541.105(d); Va. Code Ann. § 59.1-580(C).