Updates
September 26, 2023
A Potential Look Into the Future: California Issues First Draft of Cybersecurity Audit and Risk Assessment Regulations

The Board of the California Privacy Protection Agency (the CPPA) held its first meeting since July on Friday, September 8, 2023, and discussed the first public draft of cybersecurity audit regulations and risk assessment regulations.

[1] While the CPPA Board expressly announced that the drafts were for board meeting discussion purposes and that it has not started the formal rulemaking procedures yet, the first public drafts of the regulations provide a roadmap for where the CPPA Board may go, and the draft regulations would impose new and detailed compliance requirements.

The CPPA Board determined that the draft regulations will be edited prior to the next meeting, which is likely to be held in December 2023, before the regulations enter into formal rulemaking procedures. However, the CPPA Board engaged in substantive discussions about the regulations that give an indication of what the finalized regulations may look like (subject to public comment). In general, the CPPA Board stressed the importance of (1) harmony with other jurisdictions, (2) minimizing onerous requirements, and (3) the need for an economic impact analysis. Additionally, the CCPA Board expressed hope that it would present the first draft Automated Decision-Making Technology (ADMT) Regulations at the next meeting, but it will probably not enter into formal rulemaking at that time. Below, we summarize the key takeaways from the draft regulations and the latest meeting and highlight anticipated next steps in the rulemaking process.

Cybersecurity Audits

Scope

Echoing the statutory language that created the audit obligation, the draft cybersecurity regulations would require that "[e]very business whose processing of consumers' personal information presents significant risk to

consumers' security. . .complete a cybersecurity audit." Next, the draft regulations identify what would qualify as a "significant risk," breaking the risk into two sections. First, **all data brokers** (as defined under the CCPA statutory text) would constitute a "significant risk to consumers' security." Second, the draft regulations would set certain potential "significant risk" triggers based on **objective thresholds**: the volume of certain categories of personal information processed (e.g., sensitive personal information or children's data), gross revenues, or total number of employees.

During the September 8 meeting, the CPPA Board responded positively to the first portion of the draft pertaining to data brokers, suggesting that all data brokers—regardless of size or processing metrics—will likely need to adhere to this requirement. However, the CPPA Board was much more divided when it came to determining the optimal metrics for whether a business's processing constituted a "significant risk to consumers' security." In fact, none of the three proposed metrics had unanimous support from the board members. Notably, CPPA Board Member Jeffrey Worthe (attending his first CPPA Board meeting since being recently appointed) succinctly indicated a key concern with revenue as the metric: "My biggest concern is that we have small organizations that don't have [x] amount of revenue, but do process lots of data," advocating for a construction of the regulations that takes this into account. After much back-and-forth, the CPPA Board and CPPA staff agreed to table the discussion until after a fulsome economic analysis is conducted to determine the number of businesses potentially affected by the draft regulations. The scope of cybersecurity audits is expected to be an important discussion point at the next CPPA Board meeting.

Independent Auditor and Board Involvement

The draft regulations would require that cybersecurity audits must be completed "using a qualified, objective, independent professional" auditor that "may be internal or external to the business." "If the business uses an internal auditor, the auditor shall report. . .directly to the business's board of directors or governing body [or highest-ranking executive]." Notably, an internal auditor could not report to "business management that has direct responsibility for the business's cybersecurity program."

The draft regulations would also require that audit results include an attestation by the business's board of directors, governing body, or (if none) highest-ranking executive that the business did not attempt to influence the findings of the audit, and that such stakeholder has reviewed and understands the audit findings. Comments from both the CPPA Board and the public echoed support for these requirements.

Audit Requirements

The draft regulations would include a requirement that a business document and explain the business's "establishment, implementation, and maintenance of its cybersecurity program." Accompanying this requirement, a business would be required to assess and document the "safeguards the business uses to protect personal information from internal and external risks." The draft regulations contain a lengthy list of security safeguards that would be covered, and businesses would either need to address each of these safeguards or "document and explain why the component is not necessary." The list includes:

- Encryption of personal information—at rest and in transit.
- Zero trust architecture.
- Account management and access controls.
- Internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting.
- Cybersecurity awareness, education, and training.
- Oversight of service providers, contractors, and third parties.
- Incident response management.
- Business continuity and disaster recovery plans, including data recovery capabilities and backups.

The total list of potential requirements constitutes approximately six pages of the draft regulations and does not reference or provide an explicit safe harbor for any existing cybersecurity framework. The audit would be required to assess security, identify gaps, and determine steps to address any gaps. Businesses would also be required to identify any instances, worldwide, where the business was required to notify a data protection or privacy regulator of an incident, plus any other "breaches," defined with reference to California law specifically. [2] The auditor would be required to retain "all documents relevant to each cybersecurity audit" for at least five years after completing the audit.

While the regulations note that comparable audits or assessments may be used to satisfy the audit requirements, if the existing audit or assessment "does not meet all of the requirements of [the draft regulations]," the business would be required to supplement the audit or assessment. The CCPA Board did not discuss the substantive or procedural elements of this approach in the meeting on September 8.

Timing and Reporting

Any business required to complete a cybersecurity audit would have 24 months from the effective date of the regulations to complete its first audit(s) and would be required to complete an audit(s) annually thereafter. Notably, businesses would also need to annually submit a notice of compliance to the CPPA.

Risk Assessments

Scope

Following the CPRA, under the draft regulations, every business whose processing of consumers' personal information presents "significant risk" to consumers' privacy would be required to conduct a risk assessment. The regulations provide a list of activities that would be deemed to constitute a "significant risk to consumers' privacy." These activities would include:

- **Selling or sharing** personal information.
- Processing **Sensitive Personal Information** (SPI) under certain circumstances.
- Using **ADMT** in certain circumstances or processing consumer personal information in order to train artificial intelligence (AI) or ADMT.
- Processing the personal information of consumers whom the business has actual knowledge are **children** less than 16 years of age.
- Processing certain **employee** data.
- Processing the personal information of consumers in **publicly accessible places** under certain circumstances.

To aid in understanding what constitutes a "significant risk," the draft regulations also provide a list of common data processing examples that would trigger a risk assessment, such as data processing by rideshare providers, mobile dating applications, personal budgeting applications, and technology providers, among others.

Risk Assessment Requirements

The draft regulations would provide a list of 10 requirements that must be included within a risk assessment, including a short summary of the processing, anticipated benefits to consumers, anticipated negative impacts to consumers' privacy, and safeguards the business plans to implement to address any negative impacts identified. In determining negative impacts, the business would need to consider a list of 10 harms, including constitutional harms, discrimination harms, economic harms, and even psychological harms to consumers. This language drew significant commentary from the Board, and changes to the text may appear in further drafts.

The draft regulations also would require that a business weigh the risks to consumer privacy against the benefits and, if the risks to consumers' privacy outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public, the business **would not be able to engage** in processing of personal information. The risk assessments, regardless of the findings, would need to be retained for five years and provided to the CPPA upon request.

Automated Decision-Making Technology (ADMT)

The draft regulations would provide additional requirements for businesses using ADMT, focusing on businesses that process personal information to train AI or ADMT, with each term defined within the draft regulations.

These concepts constitute significant portions of the draft regulations concerning risk assessments. At the recent meeting, the CPPA Board disagreed on certain portions of this draft, including the breadth of the definitions for "Artificial Intelligence" and "Automated Decisionmaking Technology." CPPA Board Member Alastair Mactaggart noted the definition of "Artificial Intelligence" currently "covers a carburetor." In response, CPPA Board Member Vinhcent Le noted that these definitions were "adapted from the NIST standards," and that there exist other limitations within the regulations that constrain the breadth of the definitions.

Relatedly, the CPPA Board acknowledged other significant legislation in comparative jurisdictions—most notably, Europe's forthcoming AI Act—and foreshadowed that this may affect further edits to the draft regulations. The CPPA Board queried whether or not to combine these draft risk assessment regulations with the forthcoming draft regulations on usage of ADMT. Under either approach, this area promises to be a primary focus of the CPPA Board in future meetings.

Timing and Reporting

Before a business could begin a given processing activity, the business would already need to have a risk assessment conducted and then comply with specific timing requirements concerning the review of these risk assessments to ensure they remain accurate in accordance with the regulations. In the event a business already initiated a processing activity prior to the effective date of the regulations, the regulations would require businesses to conduct and document a risk assessment within 24 months of the effective date of the regulations. [3] At least every three years, a business would need to review and update the risk assessment as necessary. For ADMT risk assessments, this review would need to be conducted at least annually. These risk assessments would need to be made available to the CPPA or the attorney general upon request, as well as annually submitted to the agency in an abridged form with a certification by a designated executive that the business has complied with the requirements.

Timeline and Next Steps

CPPA Board members hinted that the next board meeting may be slightly delayed to December and stated that they hope to present the first draft ADMT regulations at that meeting, but they likely will not enter into formal rulemaking on that portion at that time. CPPA Board members also suggested that formal rulemaking for the draft cybersecurity audit and risk assessment regulations may be possible as early as the next CPPA Board meeting, although members also acknowledged that prior to entering into the formal rulemaking process, the CPPA staff must first conduct an economic analysis, and it is unclear how long that analysis will take. It is uncertain how detailed the revisions to the next draft will be, or when the public comment period will start. As such, companies should pay close attention to the draft regulations as they currently stand and begin to think through compliance steps and areas for potential public comment.

Getting Ready

Depending on the results of future CPPA Board meetings and the direction of subsequent rulemaking procedures, these draft regulations could lead to new compliance requirements and restrictions on organizations conducting businesses in California.

Our Chambers-ranked Privacy & Security team will monitor upcoming developments and collaborate with our clients to ensure their concerns are heard as the CPPA moves forward with the rulemaking processes.

Endnotes

[1] Section 1798.185(a)(15) of the CPRA directs the CPPA Board to issue regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security to (A) perform a cybersecurity audit on an annual basis and (B) submit a risk assessment to the CPPA with respect to their processing of personal information. The draft regulations set separate thresholds for (A) and (B) based on the risks to security and privacy, respectively, and thus businesses may fall under one or both requirements independently.
[2] §7123(e-g). The law references both security breaches requiring individual notification under California law, §1798.98, and "personal information security breaches" under the CCPA, § 1798.150, which are defined slightly differently. In either case, it is possible no regulatory notification had been previously required from such incidents.
[3] §7156(c). We note that while the time frame of 24 months was a tentative timeline in the current draft regulations, during the September 8 meeting, the CPPA Board expressed positive feedback regarding this time frame.

Authors

Explore more in

Privacy & Security

Related insights

Update

Trump’s FDA and USDA: Five Key Issues To Watch in 2025

Update

The Dismantle DEI Act: One Potential Blueprint for Forthcoming Attacks on DEI