Published on *The National Law Review* https://natlawreview.com

What Do the CPPA's Draft Regulations on Risk Assessments and Cybersecurity Audits Mean for Companies?

Article By:

Liisa M. Thomas

Julia K. Kadish

Kathryn Smith

The CPPA, the California regulatory body charged with enforcing CCPA, has now issued draft regulations on risk assessments and cybersecurity audits. The draft was released ahead of a public board meeting to discuss those topics (among other things).

As we have written previously, while the CPPA issued regulations to address certain parts of the CPRA amendments to the CCPA, it had not yet drafted all needed regulations. Missing were regulations to address cybersecurity audits, risk assessments, and automated decision-making technology.[1] The CPPA, in releasing these regulations in draft, emphasize their preliminary nature. Its intent, it indicated, was to facilitate public participation. Formal rulemaking has yet to begin.

Although these two are in draft form, they provide companies with an understanding of what the CPPA expects for both risk assessments and cyber audits.

- **Examples of when to conduct a risk assessment**: Under CCPA, companies must conduct a risk assessment if they process consumers' personal information in such a way that it presents significant risk to consumers' privacy or security.[2] As proposed, the draft regulations indicate that a "significant risk" is presented when selling or sharing personal information, processing sensitive information, using technology to monitor consumer behavior, and using automated decision-making technology. The regulations also give specific examples. For example, a business that offers a personal-budgeting application that collects income information that also serves targeted ads for payday loans. This is sharing, under the draft, that would merit a risk assessment.

- **Risk assessment contents:** While CCPA calls for conducting a risk assessment, it does not indicate what content to capture in that assessment. The draft regulations outline content to include, such as, *inter alia,* explaining what is being collected, how it is being used, and the "processing context." Also to include is why the processing is needed, the benefits to the business and consumer, and negative impacts on the consumer. Also to assess are the

safeguards the company will put in place to address those negative impacts.

- **Submitting the risk assessment to government authorities:** CCPA specifies that businesses submit risk assessments to the CPPA on a "regular basis." The draft regulations propose an annual submission schedule, and add that they would be submitted to on AG request.

- **Vendor contracts**: While CCPA already provides detailed provisions that must be part of vendor contracts, the draft regulations add one more. Namely, requiring that vendors assist businesses with completing risk assessments (something covered in other states, but not California). This may be another set of obligations for businesses to comply with.

- **Examples of when to conduct a cybersecurity audit**: CCPA mandates that companies must do annual cybersecurity audits if their activities present a "significant risk" to consumer privacy and security. The law indicates already that to assess risk, companies should consider their size and complexity and the nature and scope of processing activities. The draft regulations provide for more detail. To determine if an audit is needed, the regulations outline different monetary, employee, and consumer thresholds. The draft regulations also clarify that the audit can be done by an internal or external team.

- **Cybersecurity audit contents**: CCPA may require an audit, but it doesn't provide much detail in terms of what should be covered. The regulations give more detail. This includes identifying gaps and weaknesses, listing previously-identified gaps and weaknesses, and identifying corrections made. Audits under the regulations would also need to identify a person responsible for completing the audit and qualifications to do so.

- **Audit result submissions**: Under CCPA, those entities that have to conduct a cyber audit must do so annually, but there are no obligations to submit the audit to government authorities. Under the draft regulations, businesses must submit a notice of compliance to the CPPA. (The audit itself does not need to be submitted.) The notice would be a written certification of compliance -or non-compliance- covering the audit's 12-month period. If the business was not compliant, it needs to identify the areas of noncompliance and either a remediation timeline or confirmation that remediation is complete.

- **Vendor contracts**: CCPA provides detailed provisions for content to include in contracts with vendors who are collecting or processing information on the company's behalf (among other things). The draft regulations contemplate adding provisions to the existing CCPA vendor contract requirements. Namely, requiring that vendors assist businesses with completing cybersecurity audits. This may be another set of obligations for businesses to comply with.

Putting it into Practice: While rulemaking in this area is far from complete this draft is an indication of what to expect with final regulations. These drafts do not even represent the beginning of formal rulemaking. The drafts are intended to facilitate public conversations. There is no formal process for submitting comments to these drafts at this time.

FOOTNOTES

[1] 1798.185(a)(15).

[2] 1798.185(15)

National Law Review, Volume XIII, Number 257