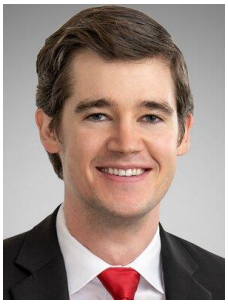
LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How Cos. Can Prep For Calif. Cybersecurity Audit Regulations

By **Caleb Skeath, Claire O'Rourke and Alexandra Bruer** (June 20, 2025, 4:43 PM EDT)


Caleb Skeath


Claire O'Rourke


Alexandra Bruer

As the California Privacy Protection Agency Board works toward finalizing regulations pursuant to the California Consumer Privacy Act, companies reviewing and preparing for compliance with the current draft of the regulations should pay particularly close attention to the potential implications of the cybersecurity audit requirement.

While the current draft would not require completion of audits until 2028 at the earliest, the draft suggests that the requirement will likely have significant effects that companies should start preparing for now.

In-scope companies, which are not limited to those headquartered in California, will likely need a significant number of resources to satisfactorily complete such an audit, and will need to generate audit reports and other documentation.

Even for entities with preexisting cybersecurity programs, the current draft suggests that a business will likely need to adjust or implement additional measures to sufficiently address the audit requirements envisioned in the draft.

While the draft has the potential to change before finalization, as it has been subject to two rounds of comments and revisions — with the latest comment period opening on May 9 and closing June 2 — companies should still anticipate the regulation to affect many aspects of their cybersecurity program.

This article describes some of these effects and complexities, as well as practical steps that companies can start taking now to prepare for compliance and reduce legal risk.

Draft Regulation Status and Overview

While the language of the cybersecurity audit regulation is not yet finalized, the current draft would require a cybersecurity audit when any of the following conditions are met: (1) deriving 50% or more of revenue from selling or sharing consumer personal information, or (2) having annual gross revenues in excess of $25 million the prior year and processing the personal information of at least 250,000 consumers or the sensitive personal information[1] of at least 50,000 consumers per year.[2]

The current draft of the regulation requires an annual audit from either an internal or external

independent party that assesses and documents how a business secures personal information and protects against unauthorized activity that results in the loss of availability of the personal information.[3]

To assess this, the audit must consider a business's cybersecurity program in light of the business's size and activities,[4] as well as 18 specifically listed components, should the auditor deem them applicable to a business's information system.[5] Many of those 18 components have additional subcategories or details on their implementation or review.[6]

Some, but not all, of the current draft's audit requirements cover topics that might be addressed in other frameworks or existing industry best practices, such as examining whether a cyber program covers authentication,[7] encryption[8] and access controls,[9] among other items.

However, other required topics, or the level of detail required for the audit, are either not covered or uncommon in industry standards or other laws. For example, auditors are supposed to assess (1) antivirus and antimalware protections,[10] and (2) limitations on ports and protocols.[11] These aspects of a cyber program are not frequently identified as stand-alone areas of assessment.

In addition, the draft regulations include assessment of other cybersecurity practices, such as masking and password specifications, that are uncommon to be prominently featured in statutory or regulatory requirements, or even in common cybersecurity frameworks.

Under the current draft regulations, businesses must certify each year under the penalty of perjury that they are in compliance with the annual audit requirement in the current version of the draft regulations.

While they do not need to submit the audit itself in the current draft, the CPPA board can acquire copies of audit materials through its broader compliance audit right.[12] Comments have expressed concerns about the confidentiality of these sensitive materials.

The draft allows for a phase-in of the audit requirements based on size, going from 2028 to 2030.[13]

Preparing for Audit Requirements

Companies will need to prepare both for the audit itself and for a compliant cybersecurity program that can pass the audit. The earliest wave of covered companies will need to file their first audit certification no later than April 1, 2028.[14]

For those included in that first group of covered entities, the first audit must cover calendar year 2027, which means a business should consider assessing, no later than 2026, its cybersecurity program and addressing anticipated program gaps that would hamper its ability to have a successful audit.

While the CPPA works toward a final version of the cybersecurity audit regulation, it is apparent from the current draft that the regulation will likely have significant effects on the cybersecurity programs and practices of a wide variety of companies. Companies should start preparing for these effects well in advance.

To do so, companies could consider taking the following steps.

Monitor the progress and content of the draft audit regulation.

As noted above, the draft regulation is not yet final and could change. Companies should not only evaluate whether they might be subject to the regulations as currently drafted, but also monitor for updates to the draft regulations as the CPPA works to finalize them. If of interest, entities might also want to maintain awareness of opportunities to provide feedback on the draft regulations.

In particular, companies should consider closely monitoring for any changes on the scope of entities subject to the requirement, the timing for implementation of this requirement, and how prescriptive the substance of the cybersecurity audits must be, as those might have significant effect on the cost, nature and timing of required actions to prepare for compliance.

Do not assume compliance based on adherence to industry standards.

While the CPPA audit regulation is one of several detailed cybersecurity frameworks recently enacted (or in the process of being enacted), such as the Network and Information Systems Directive 2 in the European Union or the New York Department of Financial Services' cybersecurity regulations, compliance or alignment with another framework or industry standard (such as the National Institute of Standards and Technology's Cybersecurity Framework) will not necessarily equate to compliance with the audit regulation, as currently drafted.

Instead, the current draft will likely require in-scope entities to build additional California-specific measures on top of existing programs and cybersecurity audits.

Review existing cyber programs to identify potential gaps.

As the CPPA nears a final version of the audit regulation, companies that are likely to be in scope for the requirement should consider reviewing their existing cyber program against the proposed California requirements.

To the extent that a business is already reviewing its cybersecurity program, whether as part of an existing review cycle or to prepare for other recently implemented cybersecurity requirements (such as NIS 2), it could consider folding in elements of the current draft audit requirement into that review.

In addition, as a review or assessment will likely involve sensitive discussions of legal risk and compliance, companies should consider conducting reviews or assessments under privilege at the direction of counsel to protect these materials from disclosure.

Update existing cyber programs to address gaps.

Based on the review of its existing cyber program, a business will need to decide where its program differs from the California requirements and whether it needs to close those gaps.

For gaps it determines it should address, the security team and business will need to work together to implement new California-driven measures. However, companies might not need to address all identified gaps, as the current draft regulation suggests that certain elements might not be required if they are not "applicable to the business's information system."[15]

Update auditing schedule and plans.

A business should review its existing audit calendar and processes to see how to efficiently build in this review. It should also consider whether it wants the review to be done internally or externally.

External auditors often receive more requests than they can fill in the wake of new auditing requirements. If a business has a preferred auditor, it should be timely in engaging the auditor's services.

Review for consistency with other cyber statements.

A business may be required to present or affirm details related to its cybersecurity program in various contexts, such as annual Form 10-K filings or reports submitted under security-related settlements with state and federal regulators.

Often, these other presentations review the same areas of a cyber program or require certification of similar components. Businesses should build in coordination time and processes to help with consistency in cyber program presentation and certifications across legal filings, including the California cyber audit certification.

Conclusions

While the California cyber audit provisions still have potential to evolve before finalization, nearly all aspects of an organization's cybersecurity program will be touched by them once they are in place.

Reviewing, preparing and monitoring now will help with the eventual compliance burden and reduce potential legal risk in California and elsewhere from having to conduct and document cybersecurity audits.

Caleb Skeath is a partner, and Claire O'Rourke and Alexandra Bruer are associates, at Covington & Burling LLP.

[1] The draft regulation contains a definition for "sensitive personal information." See Proposed Regulations on CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decisionmaking Technology (ADMT), and Insurance Companies, § 7001(bbb) (May 9, 2025).

[2] See id. at § 7120.

[3] See id. at § 7122(a).

[4] See id. at § 7123(b)(1).

[5] See id. at § 7123(b)(2).

[6] See id. at § 7123(c).

[7] See id. at § 7123(c)(1).

[8] See id. at § 7123(c)(2).

[9] See id. at § 7123(c)(3).

[10] See id. at § 7123(c)(9).

[11] See id. at § 7123(c)(11).

[12] See id. at § 7124.

[13] See id. at § 7121(a).

[14] See id.

[15] See id. at § 7123(b)(2).