Cooley

Tell Them How You Feel CPPA Opens Public Comment Period for Cybersecurity Audit Regulation

May 20, 2025

Certain businesses subject to the California Consumer Privacy Act (CCPA) will soon be required to conduct annual cybersecurity audits, and the California Privacy Protection Agency (CPPA) is once again soliciting feedback on what cybersecurity audits should look like. On May 9, the CPPA opened the formal public comment period on its latest modifications to several proposed regulations, including those regarding cybersecurity audits. This round of modifications clarifies when the audit requirement (if passed) will go into effect, clarifies which businesses will be subject to the audit requirements, introduces the requirement of a documented cybersecurity audit report and expands upon the requirement to submit a certification of completion to the CPPA. The CPPA is accepting comments on its modifications until June 2, 2025.

How did we get here?

This formal rulemaking is a long time in the making. It traces back to a statutory directive in the CCPA, which was signed into law in 2018. The CCPA requires the CPPA to issue regulations "requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security, to … [p]erform a cybersecurity audit on an annual basis.[1]

The CPPA's initial invitation for preliminary comments on cybersecurity audits and other topics opened more than two years ago on February 10, 2023. From there, the CPPA spent more than 18 months developing a formal rulemaking package, which it approved on November 8, 2024. It then accepted another round of public comments during an extended public comment period that ran from November 22, 2024, through February 19, 2025.

This extensive rulemaking activity most recently culminated in the latest modifications, which the CPPA published on May 9.

Who would be subject to the proposed cybersecurity audit requirement and when?

This round of modifications did not change the basic criteria for determining which businesses are required to complete an audit, but it did provide new information on how and when these criteria are to be applied.

Businesses must conduct cybersecurity audits if their "processing of consumers' personal information presents significant risk to consumers' security," as laid out in the CCPA. The draft regulations say this significant risk is present if the business (1) "derives 50 percent or more of its annual revenues from selling or sharing consumers' personal information"[2] or (2) has "gross annual revenues in excess of $25 million in the preceding calendar year,"[3] and (a) "processed the personal information of 250,000 or more consumers or households in the preceding calendar year" or (b) "processed the sensitive personal information of 50,000 or more consumers in the preceding calendar year."

New additions to the draft regulations clarify when that test will be applied and when the requirement will become effective for different sized businesses. Larger businesses (defined in terms of gross annual revenues) will see an earlier effective date, and smaller businesses will enjoy a later effective date.

- **Businesses with annual revenues in excess of $100 million as of January 1, 2027.** These businesses will be required to complete their first cybersecurity audit by April 1, 2028. The audit must cover the period from January 1, 2027, to January

1, 2028.

- **Businesses with annual revenues between $50 million and $100 million as of January 1, 2028.** These businesses will be required to complete their first cybersecurity audit by April 1, 2029. The audit must cover the period from January 1, 2028, to January 1, 2029.
- **Businesses with annual revenues of less than $50 million.** These businesses will be required to complete their first cybersecurity audit by April 1, 2030. The audit must cover the period from January 1, 2029, to January 1, 2030.

After April 1, 2030, businesses will be required to complete a cybersecurity audit if, on January 1 of a given year, the business meets the significant risk criteria laid out above. In years for which that is the case, the business will be required to complete a cybersecurity audit by April 1 of the following year, covering the period of that year.

This staggered approach to rolling out the audit requirement gives businesses some time to bring their cybersecurity practices up to par with the proposed regulation's requirements and gives the market time to develop cost-effective auditing services.

What does the latest version of the cybersecurity audit regulations require?

A notable addition to the draft regulation is that businesses must not only audit their cybersecurity practices but also produce an audit report documenting the audit's findings. Previously, the regulations referenced certain requirements of the audit but did not impose such prescriptive requirements on how the audit's findings are to be organized.

The regulations lay out detailed requirements for what the audit report must contain, including but not limited to:

- A description of the business's information systems and relevant policies, procedures and practices, along with the audit's criteria, the specific evidence examined as part of the assessment, and an explanation of why the audit of that evidence justifies the auditor's findings.
- Identification of applicable cybersecurity components, including but not limited to those related to authentication, encryption, account management and access controls, inventory management, secure configurations and network monitoring, and defenses.
- Identification of relevant gaps and weaknesses, along with the business's plan to address those gaps and weaknesses.
- Any corrections or amendments to prior audit reports.
- The names and titles of up to three qualified individuals responsible for the business's cybersecurity program.

The modifications also would impose more detailed certification requirements following annual audits. In keeping with previous drafts of the regulations, the modified regulations require businesses to submit a certification of completion to the CPPA following each audit they conduct. The modifications set forth additional requirements for this certification, including but not limited to:

- A submission deadline of April 1 following any year that a cybersecurity audit is required.
- The signature of a member of the business's executive management team.
- Submission to the CPPA through its website, including:
    - The business's name and contact information.
    - A statement of completion.
    - The time period covered by the audit.
    - An attestation of the truth and correctness of the certification.
    - The name and title of the individual submitting the certification.

Other portions of the proposed regulation received less drastic modifications since previous drafts.

For example, the modifications still require auditor independence but no longer require board oversight of the audit and auditor independence. The audit must be completed by an independent auditor, which may be an individual internal or external to the business. The modifications require that internal auditors report to a member of the business's executive management team (rather than reporting to the board, governing body or highest-

ranking executive), who does not have direct responsibility for the business's cybersecurity program. Likewise, the audit report must be provided to a member of the business's executive management team (rather than to the board, governing body or highest-ranking executive), who has direct responsibility for the business's cybersecurity program.

Regarding documentation and recordkeeping, the modifications now require the business, in addition to the auditor, to retain all documents relevant to the audit for a period of at least five years.

Finally, the modified regulation still allows businesses to "piggyback" and utilize a cybersecurity audit conducted for a different purpose to satisfy the regulation, so long as that audit, on its own or through supplementation, meets all the CPPA regulation's requirements. The modifications now provide a representative example, citing that a business could use a cybersecurity audit assessing compliance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0 if that audit meets all the regulation's requirements.

What kinds of sources informed the proposed cybersecurity audit regulations?

California law requires state agencies to make available any materials added to the rulemaking file after the notice of proposed action is published, if they rely on those materials.[4] This requirement helps give insight into what may have motivated some of the changes the agency made.

The materials disclosed by the CPPA in relation to the modifications include the NIST Catalog of Problematic Data Actions and Problems (PDAP Catalog).[5] As its name implies, the PDAP Catalog lists illustrative problematic data actions a business might engage in, such as insecurity, and the kinds of problems those actions could cause, including dignity loss, economic loss, physical harm or loss of trust. The CPPA may see cybersecurity audits as a way to encourage businesses to reflect on and bolster their cybersecurity practices, and in so doing reduce the likelihood of data-related harms coming to pass.

Comment period

The CPPA is accepting comments on its proposed modifications to the proposed cybersecurity audit regulations and other topics of regulation until June 2, 2025. It accepts comments via email (be sure to include "Public Comment on CPPA Updates, Cyber, Risk, ADMT and Insurance Regulations" in the subject line) and by mail at:

> California Privacy Protection Agency
> Attn: Legal Division – Regulations Public Comment
> 400 R St., Suite 350
> Sacramento, CA 95811

Cooley law clerk Emma Plankey also contributed to this alert.

Notes

1. Cal. Civ. Code § 1798.185(a)(15)(A).
2. Cal. Civ. Code § 1798.140(d)(1)(C).
3. Id at § 1798.140(d)(1)(A).
4. See Cal. Gov. Code § 11347.1.
5. Download the PDAP Catalog on this NIST resource page.

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act

or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

Key Contacts

Kristen Mathews **New York**	**kmathews@cooley.com**

This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.