FACT SHEET

DRAFT CYBERSECURITY AUDIT REGULATIONS

CPPA

CYBER

The California Consumer Privacy Act (CCPA) directs the Agency to make rules requiring certain businesses to complete yearly cybersecurity audits. The Agency has drafted cybersecurity audit regulations but has not yet started the formal rulemaking process. This fact sheet explains the draft regulations to help people understand and participate in the rulemaking process. These draft rules are *not* in effect and are subject to change.

WHO would need to complete a cybersecurity audit?

A "business" that must comply with the CCPA[1] and meets either of the following criteria:

1 The business made 50% or more of its annual revenue the prior year from selling or sharing consumers' personal information.

OR

2 The business made over $28 million[2] in annual gross revenue last year **AND**

- Collects, uses, discloses, retains, or otherwise processes the personal information of 250,000 or more consumers, **OR**
- Collects, uses, discloses, retains, or otherwise processes the "sensitive personal information"[3] of 50,000 or more consumers.

HOW would a business complete a cybersecurity audit?

1 Select an auditor.

2 Provide all information the auditor asked for and not hide important facts from them.

3 Present the audit results to the most senior individuals in the business responsible for its cybersecurity program.

4 Submit a certification of completion to the Agency.

CYBER

WHO could the auditor be, and WHAT would the auditor have to do?

- The auditor would have to be qualified, unbiased, and independent, and use professional auditing procedures and standards.
- The auditor could be someone working in the business or outside of the business. If an auditor were internal, they would have to report to the business's board, governing body, or highest-ranking executive who does not have direct responsibility for the cybersecurity program.
- Whether working in the business or not, the auditor would have to:
  - Determine which systems would need to be audited and how they would be assessed;
  - Independently review documents, conduct tests, and interview people to support audit findings; and
  - Certify that they completed an independent and unbiased audit.

WHAT would a cybersecurity audit include?

- A description of the systems being audited.
- The information the auditor used to make decisions and why it supported their findings.
- An assessment of how the business protected personal information through its cybersecurity program.
- A description of how the business followed its own cybersecurity policies and procedures.
- A description of the gaps and weaknesses of the cybersecurity program, and how the business plans to address them.
- A description or sample copy of data-breach notifications that were sent to consumers or agencies, and related information and fixes.

Common ways a business protects personal information include:

- Multifactor authentication
- Encryption
- Account management and access controls
- Inventorying and managing personal information and the business's information system
- Cybersecurity training
- Incident-response

- The dates that the cybersecurity program was reviewed and presented to the most senior individuals in the business responsible for its cybersecurity program.
- A certification that the business did not influence the auditor's decisions or assessments, and that the business reviewed and understood the audit findings.

How would a business complete a cybersecurity audit if it used service providers or contractors to provide the business's cybersecurity services?

The business's service provider or contractor would be required to give the business the information needed to carry out the business's cybersecurity audit. The business's auditor could get information from them as part of the business's cybersecurity-audit process.

WHEN would a business have to complete its cybersecurity audit?

A business would have 24 months to complete its first cybersecurity audit and submit its certification of completion to the Agency. It would then complete a cybersecurity audit and submit a certification each following year.

What if a business completed a cybersecurity audit or assessment for another purpose, or had a cybersecurity certification? Would that count toward its CCPA annual cybersecurity audit?

A business would not have to redo the same cybersecurity audit. However, if the audit, assessment, or certification did not meet all of the requirements in the draft regulations, the business would have to add to it as needed.

[1] The CCPA generally does not apply to nonprofit organizations or government agencies. For more information, *see* "Does My Business Need To Comply With The CCPA?" fact sheet at https://cppa.ca.gov/resources.html.

[2] This includes the legally required increase to account for the increase in the Consumer Price Index. *See* Draft Update to Existing Regulations, March 2023, at § 7005(b)(1), available at https://cppa.ca.gov/meetings/materials/20240308_item4_draft_update.pdf.

[3] Sensitive personal information includes things like Social Security numbers, financial information, precise geolocation, health information, and children's personal information. For more information, *see* Civil Code § 1798.140(ae); Draft Update to Existing Regulations, March 2023, at § 7001(ii) (including the addition of "[p]ersonal information of consumers that the business has actual knowledge are less than 16 years of age" to the definition), available at https://cppa.ca.gov/meetings/materials/20240308_item4_draft_update.pdf; and "What is Personal Information?" fact sheet, available at https://cppa.ca.gov/resources.html.

Supporting Resources: Civil Code § 1798.185(a)(15)(A); Proposed Rulemaking Draft: Cybersecurity Audit Regulations, December 2023, available at https:/cppa.ca.gov/meetings/materials/20231208_agenda_item2a_cybersecurity_audit_regulations_clean.pdf.