Articles + Publications | April 1, 2024

California's Draft Proposed Regulations on Cybersecurity Audits

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Alexander R. Cox

RELATED OFFICES

Hartford

Although not yet the subject of the formal rulemaking process, the California Privacy Protection Agency (the "CPPA") has released draft proposed regulations for cybersecurity audits required by Section 1798.185(a)(15)(A) of the California Consumer Privacy Act, as amended by the California Privacy Rights Act (the "CCPA").[1] These draft proposed regulations on cybersecurity audits would cover one of the three remaining areas for which the CPPA is required by the CCPA to promulgate regulations.[2]

Businesses that would be subject to the cybersecurity audit requirements discussed below should begin now to plan and schedule cybersecurity audits, even though the draft proposed regulations are subject to change, and the formal rulemaking process has not formally begun. It can be expected that qualified auditors will be in high demand for these services, and in short supply with limited capacity.

Effective Date. It is important to note that the draft proposed regulations would require a business (as defined by the CCPA) to complete its first annual cybersecurity audit within 24 months from the effective date of the regulations. Given that formal rulemaking on this subject has not yet begun, businesses will have a minimum of 30 to 36 months from now to complete the first cybersecurity audit, with annual audits required thereafter.

Scope. Under the draft proposed regulations, a business otherwise subject to the CCPA will be subject to the cybersecurity audit requirement only if it (a) derives 50% or more of annual revenues from selling or sharing consumers' (*i.e.*, California residents') personal information, or (b) has $25,000,000 or more in gross revenue the preceding year and processed in the preceding calendar year any of the following: (i) personal information of 250,000 or more consumers or households; (ii) sensitive personal information of 50,000 or more consumers or households; or (iii) personal information of 50,000 or more consumers known to be under 16. Other businesses would not be subject to the cybersecurity audit requirement, according to the current draft proposed regulations.

Cybersecurity Audit Requirements. Cybersecurity audits will be required to satisfy several requirements.

Auditor Independence. In accordance with Under Section 7122 of the proposed draft regulations, the auditor can be either internal or external auditors, but must be independent, using procedures and standards generally accepted in the profession of auditing, exercising objective and impartial judgment on all issues within the scope of

the cybersecurity audit, and free to make decisions and assessments without influence by the business, including its owners, managers or employees. The auditor would not be permitted to participate in activities that would compromise or appear to compromise independence, including by participating in the business activities that the auditor may assess, including developing procedures, or making recommendations regarding the business's cybersecurity program. If the auditor is internal to the business, the auditor's report must be issued directly to the business's governing body, which will evaluate the auditor's performance and set the auditor's compensation.

Scope of the Audit. The cybersecurity audit would be required to identify, assess, and document the business's cybersecurity program and related policies and procedures appropriate to the business's size and complexity and the nature and scope of its processing, covering the following 18 specific elements, as applicable:

A. authentication, including multi-factor authentication and passwords;
B. encryption of personal information at rest and in transit;
C. zero trust architecture;
D. account management and access controls;
E. information assets inventory and management;
F. secure configuration of hardware and software, including patch and change management;
G. internal and external vulnerability scans, penetration testing, and vulnerability disclosure and reporting;
H. audit log management;
I. network monitoring and defenses;
J. antivirus and antimalware;
K. systems segmentation;
L. limitation and control of ports, services and protocols;
M. cybersecurity awareness, education and training;
N. secure development and coding best practices;
O. oversight of service providers, contractors and third parties;
P. retention and disposal;
Q. incident response; and
R. business continuity and disaster recovery.

Under the draft proposed regulations, the audit would assess these components, identify and describe gaps and weaknesses, document the plan to address gaps and weaknesses, include the titles of individuals responsible for the cybersecurity program, and include the date of presentation to the governing body. The audit will require the identification and description of past notifications to consumers and government agencies, with a copy of the notification letters.

Annual Certification. The draft proposed regulations would require each business required to complete a cybersecurity audit to provide the CPPA an annual certification of compliance with the cybersecurity audit requirements, or a written acknowledgement that the business did not fully comply, identifying all requirements that were not met, and a remediation timeline.

—

[1] CPPA December 8, 2023 Board Meeting, Meeting Materials, Agenda Item 2(a), available at https://cppa.ca.gov/meetings/materials/20231208_agenda_item2a_cybersecurity_audit_regulations_clean.pdf

[2] The other two areas are risk assessments (CCPA Section 1798.185(a)(15)(B)), and automated decisionmaking (CCPA Section 1798.185(a)(16)).

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber