CPPA Proposed Rulemaking Package Part 1—Cybersecurity Audit

December 3, 2024

On November 22, 2024, the California Privacy Protection Agency (the "CPPA") opened the formal public comment period for its recently approved formal proposed rulemaking package for annual cybersecurity audits, automated decision-making technology, privacy requirements, insurance companies' obligations, and other updates to existing regulations (the "Draft Regulations"). The Draft Regulations fulfill the CPPA's mandate under the California Consumer Privacy Act (the "CCPA") to provide rules on these topics. This blog post is the first in a series that discuss the Draft Regulations, starting with the new annual cybersecurity audit requirements.

The cybersecurity audit provisions under the CCPA include both procedural "how" obligations, as well as substantive "what" requirements for reasonable cybersecurity. If adopted, the cybersecurity audit requirements would join the New York Department of Financial Services ("NYDFS") Part 500 in the developing field of prescriptive mandatory cybersecurity audits in state regulations. Previously, such audits were required only for a very narrow group of businesses, for example, those who participated in the payment card industry (e.g., Payment Card Industry Data Security Standard) or served as a government contractor for cloud products and services (e.g., the Federal Risk and Authorization Management Program).

The CPPA's Rulemaking Mandate for Cybersecurity Audits

The CCPA directed the CPPA to make rules requiring certain businesses to complete annual cybersecurity audits. Per the CCPA, the regulations must include "the scope of the audit and establishing a process to ensure that audits are thorough and independent." The Draft Regulations are based on the outputs from several years of preliminary rulemaking activities, including written public comments and targeted stakeholder sessions.

The Draft Regulations create a new Article 9, "Cybersecurity Audits." While the substantive components in the section largely reflect those of previous drafts, the Draft

Regulations clarify the thresholds for applicability and the means of performing the audit.

Covered Businesses

The CPPA has determined that businesses that meet either of the following thresholds are engaged in the processing of California residents' ("consumers") personal information in a way that presents *significant risk* to consumers' security, and therefore must conduct an annual cybersecurity audit:

- derived 50% or more of its annual revenue from selling or sharing consumers' personal information in the previous calendar year; or
- made over $25 million in gross annual revenue and processed either (a) the personal information of 250,000 or more consumers or households or (b) the sensitive personal information of 50,000 or more consumers in the preceding calendar year.

"Sensitive personal information" includes biometric information, information that would trigger a data breach notification under California law (e.g., Social Security number), contents of communications where the business is not an intended recipient, and information belonging to consumers that the covered business knows to be less than 16 years of age. In practice, this will sweep in businesses that process large amounts of relatively innocuous data, and we anticipate the CPPA will receive comment letters suggesting that it tether the cybersecurity audit requirement to risk, rather than mere volume.

Cybersecurity Audit Requirements

Thoroughness and Independence

The Draft Regulations prescribe in detail how the cybersecurity audit must be conducted, including relevant standards for thoroughness and independence. Specifically, the Draft Regulations would require that:

- Auditors be sufficiently qualified, objective, and independent.
- Auditors be internal or external to the organization but must exercise objective and impartial judgment, not be subject to the business's influence, and not participate in

activities that compromise independence (e.g., developing procedures or making recommendations regarding the business's cybersecurity program).

- If internal auditors are used, they must report directly to the board or, if none exists, the highest-ranking executive that does not have direct responsibility over the cybersecurity program. The internal auditor's performance evaluation and compensation shall be conducted by the board or the aforementioned highest-ranking executive.

- Audit findings need to be based on specific evidence (i.e., documents reviewed, sampling and testing performed, and interviews conducted) and the audit cannot rely primarily on assertions or attestations by the business's management.

Substantive Requirements

In addition to prescribing how the audit must be conducted, the Draft Regulations provide 18 enumerated components of a business's cybersecurity program that the cybersecurity audit must cover, as applicable; if inapplicable, the cybersecurity audit must document and explain why the safeguard is unnecessary for the business's protection of personal information, and how existing safeguards provide equivalent security. The Draft Regulations also make clear that businesses are not restricted to only auditing the enumerated components.

Specifically, the Draft Regulations would require that the cybersecurity audit review a business's policies, procedures, and practices on authentication, encryption, zero-trust architecture, access control measures, data and asset inventory, vulnerability management, logging & network monitoring, antivirus and antimalware protections, network segmentation, limitation and control of ports, services, and protocols, employee training, incident response and business continuity, secure development, vendor oversight, and data retention and disposal.

Within the list of components, the Draft Regulations provide granular examples of what is required. For example, the Draft Regulations expand on network monitoring requirements, specifying that this component "include[s] the deployment of bot-detection and intrusion-detection and intrusion-prevention systems" and "data-loss prevention systems." Similarly, for access control requirements, the Draft Regulations reference least privilege access, restricting the number of privileged accounts, and restricting and monitoring physical access to personal information.

For each of the 18 substantive components described above, the Draft Regulations also require the cybersecurity audit to:

- identify gaps or weaknesses in the cybersecurity program and document the plans to address them;
- address the status of any previously identified gaps and weaknesses;
- identify any corrections or amendments to any prior audits; and
- include any sample consumer or regulatory notifications made in connection with any unauthorized access or disclosure of personal information required by any applicable privacy laws, and corresponding detailed descriptions of the same.

Certification and Timing

Although copies of the cybersecurity audits need not be shared with the CPPA, the Draft Regulations impose a certification obligation on auditors and covered businesses, including:

- The auditor must certify that their work primarily relied on evidence and not on representations by management, as well as the fact that the business was compliant for the past 12 months. A member of the business's board (and if none exists, the highest-ranking executive responsible for overseeing the cybersecurity audit) must certify that they have reviewed and understood the content of the audit.
- Businesses will have 24 months from the effective date of the proposed regulations to complete their first audit (but note that the audits apply to the past 12 months), with subsequent audits due annually thereafter.
- When completed, businesses must upload the audit to the CPPA's website, identifying the 12 months covered by the audit.
- The auditor must retain all documents relevant to each cybersecurity audit for a minimum of five years after completion of the audit.

Duplicate Audits

The Draft Regulations contemplate that a business can rely on cybersecurity audits completed for other business purposes, but only to the extent that the other audits meet all the requirements of the Draft Regulations. In practice, this may drive businesses to reorient their auditing practices or modify regularly scheduled cybersecurity audits to ensure that they meet the requirements of the Draft Regulations.

What's Next?

While the CPPA's rulemaking on cybersecurity audits is in its early stages, the Draft Regulations have the potential to heighten regulatory expectations for what constitutes reasonable cybersecurity measures. As such, even companies that do not do extensive business in California may wish to note what the Draft Regulations propose and consider moving towards compliance with the substance of these proposals.

The formal public comment period concludes on January 14, 2025, which reflects an extension to the statutory 45-day comment period to accommodate the winter holidays and "give all interested parties sufficient time and capacity to weigh in on this important rulemaking package." Any subsequent substantive changes to the Draft Regulations would trigger an additional 15-day comment period.

Practical Considerations

Although couched as cybersecurity practices that the audit must cover, the enumerated components appear to lay out substantive cybersecurity practices that the CPPA expects of covered businesses. The CPPA indicates as much in its Initial Statement of Reasons for the Draft Regulations, as it explains "[t]hese 18 components … align with the guidance provided in prominent cybersecurity frameworks and resources, such as the NIST Cybersecurity Framework, the Center for Internet Security Critical Security Controls, and guidance from the FTC and the Attorney General." As such, the substantive requirements for cybersecurity audits, if adopted as drafted, would set new standards for what constitutes reasonable cybersecurity measures in California and beyond. For businesses proactively considering their regulatory and cybersecurity posture, the following areas may be helpful to consider:

- **Existing Coverage**. The proposed articles permit audits undertaken to meet other regulatory standards, provided they either satisfy the CCPA's requirements or can do so with supplementation. Businesses that already follow standards such as ISO27001 or SOC2 may already have significant coverage under their existing cybersecurity audits.

- **Equivalent Controls**. Components of the proposed CCPA audit may be omitted from a business's audit, provided that the cybersecurity audit explains how existing safeguards provide at least equivalent security. If a company excludes a component from its audit, the audit documentation should (1) reflect why the company believes the component is not necessary for the protection of personal information and (2) describe how the preexisting safeguards provide at least equivalent security.

- **Training as a Regulatory Expectation**. The proposed CCPA article mandates training as an auditable component of a cybersecurity plan. In jurisdictions with similar mandates, inadequate training has been explicitly cited by regulators as a factor in their final determinations. Given the heightened expectations and independent audits for efficacy, businesses may wish to supplement their general training with in-depth practical exercises, such as phishing tests and tabletop exercises.

- **Documentation**. The audits require enhanced documentation of a business's cybersecurity program, including identified "gaps or weaknesses" and the status of any efforts to address or mitigate the corresponding risks. As businesses are conducting CCPA audits, internal technical, business, and audit teams, if applicable, should make sure that either in-house legal or outside counsel is engaged in the creation of any documentation relating to the audit. Counsel plays a key role in ensuring that documentation facilitates compliance while also reducing the risk that such documentation is used as a regulatory or litigation roadmap for enforcement or settlement.

- **Plan for Integration**. Under the proposed changes, members of management facilitate, review, and certify their understanding of the audit. Businesses may want to consider how to integrate these requirements into their organizations' existing workflows within the timelines proposed by the CCPA.

* * *

Please do not hesitate to contact us with any questions.

Avi Gesser
Partner, New York
+1 212 909 6577
agesser@debevoise.com

Matt Kelly
Counsel, New York
+1 212 909 6990
makelly@debevoise.com

Johanna N. Skrzypczyk
Counsel, New York
+1 212 909 6291
jnskrzypczyk@debevoise.com

H Jacqueline Brehmer
Associate, San Francisco
+1 415 738 5703
hjbrehmer@debevoise.com

Ned Terrace
Associate, New York
+1 212 909 7435
jkterrace@debevoise.com

Mengyi Xu
Associate, San Francisco
+1 415 738 5725
mxu@debevoise.com

Amer Mneimneh
Law Clerk, New York
+1 212 909 6023
amneimneh@debevoise.com