Debevoise
& Plimpton

Debevoise In Depth

NYDFS Publishes Official Amendments to Its Cybersecurity Regulation

November 11, 2022

On November 9, 2022, the New York Department of Financial Services ("NYDFS") announced the publication of the official proposed amendments to its 2017 Cybersecurity Regulation 23 NYCRR 500 ("Proposed Amendments"). This announcement follows a highly active pre-proposal comment period, during which industry stakeholders shared their thoughts with the NYDFS on the changes under consideration, which we covered here for an Overview, here for a Q and A, and during a webcast. The 60-day public comment period to the Proposed Amendments ends on January 9, 2023. In this blog post, we discuss our initial observations on significant changes between the new release and the pre-proposal.

Highlights of what we learned from the revisions:

- NYDFS took the time to ingest comments and clarify interpretations, so the next round of comments is very important.
- The Revised Proposal softens the definition of Class A companies.
- The Revised Proposal softens the prescriptive requirements around key controls, bringing back some of the risk-based elements of the existing Part 500.
- NYDFS understands that the implementation periods for some technical elements were too aggressive and has softened those requirements.

Revised Definition of Class A Companies and of Other Key Terms

In the pre-proposal, NYDFS created a new category of companies called "Class A" companies. Class A companies were defined as those with over 2,000 employees as part of the covered entity and its affiliates OR those companies with over $1 billion in gross annual revenues averaged over the last three years for the covered entity and affiliates. The Proposed Amendments revised the definition of Class A Companies. The new formulation appears designed to reduce the scope of the Class A Companies.

- As a threshold, the Covered Entity must have an **in-state (New York) gross annual revenue** of "at least $20,000,000" "in ***each of*** **the last two fiscal years** from business operations of the covered entity and its affiliates." This may exclude some international banks with small branches in New York from the Class A definition.

- If the $20 million revenue in New York threshold is met, then:

  - The Proposed Amendments now clarify that a company would be a Class A if it **has 2,000 employees** as an ***average*** **over the last two fiscal years**, still accounting for the covered entity and affiliates.

  - Alternatively, a company can be Class A if the **global gross annual revenue threshold of $1 billion** is met in ***each of*** **the last two fiscal years**, as opposed to being an average of the two.

This revised definition addresses Question 1 from our webcast by clarifying when a small NY branch of a larger overseas company might be considered a Class A Company. In addition, the Proposed Amendments:

- Remove the possibility that an internal audit can satisfy an "independent audit" by making clear that an audit must be conducted by an external auditor;

- Carve out "governmental entity" from the definition of a "third party service provider";

- Change references to the CEO for requirements such as compliance certification to the "highest-ranking executive at the covered entity" which clarifies an ambiguity in the pre-proposal draft that these requirements might adhere to CEO's of parent companies of Covered Entities that themselves did not have CEOs.

Emphasis on Certain Key Cybersecurity Domains

Certain revisions throughout the Proposed Amendments reflect NYDFS's enhanced focus on key cybersecurity domains and industry best practices. For example:

- **Cybersecurity policies and procedures** – [500.3] the addition of data "retention," systems and network "monitoring," "security awareness and training," and incident "notification" to the list of areas that must be addressed (to the extent applicable) by the covered entity's cybersecurity policies based on its risk assessment.

- **Incident Investigation** – [500.16] the addition of an explicit reference to the investigat[ive] aspects of an incident response plan.

- **Annual Training and Testing of Incident Response Plan** – [500.14 & 500.16(d)(1)] the addition of a minimum annual cadence to (1) the training requirement with an explicit reference to social engineering exercises (expansion from just "phishing"); and (2) the testing requirement for incident response plans (the requirement for CEO participation is replaced with that of the "highest-ranking executive" of the Covered Entity).

- **Backups** – [500.16(e)] the change of the backup requirement from an action-oriented one (network isolation) to a goal-oriented one (adequate protection from unauthorized alterations or destruction).

- **Remedial Measures –** [500.17(b)(1)(ii)(d)] the addition of "remediation plans and timeline for their implementation" as a required element of a covered entity's written annual certification.

Softening of Certain Prescriptive Governance Requirements

The Proposed Amendments remove the CISO independence requirement in the pre-proposal draft and adjust the mandatory nature of the additional board reporting requirement.

- The Proposed Amendments require the CISO to have authority and "the ability to direct sufficient resources to implement and maintain a cybersecurity program" but remove the requirement for CISO independence. This appears to be more practical for the purposes of effective program implementation and oversight without getting into locations on an org chart.

- The Proposed Amendments further amend the CISO's annual reporting to the Board or equivalent. The CISO still needs to consider a number of factors in developing a report, but the report no longer needs to include discussions of each such factor and does not need to include plans for remediating inadequacies.

- Finally, the Proposed Amendments seem to clarify that the Board's role is to "exercise oversight and provide direction to management on … cybersecurity risk management." Covered Entities still need to report material issues found in the vulnerability management program to the "senior governing body."

Clarifications on Penetration Testing, Vulnerability Management & Access Controls

The Proposed Amendments:

- Clarify that the required **penetration testing** (1) includes both external network penetration testing (from outside the information systems' boundaries) and internal network penetration testing (from inside the information systems' boundaries); but (2) can be conducted by a qualified independent party regardless of affiliation (can be both internal and external). [500.5(a)(1)]

- Add an explicit requirement for **vulnerability scans** to cover the entire environment, whether by automated or manual means. While a specific frequency for such scans is not mandated, the Proposed Amendments reflect the expectation for a risk-based cadence and the assumption that such scans will be conducted after any major system changes. [500.5(a)(2)]

- Mandate that **user access privileges** be reviewed at least annually and terminated upon employee departures. [500.7(a)(4) & (6)]

- Replace the pre-proposal requirement for "strong, unique passwords" with a requirement to **implement a "written password policy" meeting "industry standards."** [500.7(b)]

- Clarify the scope of the **access control** requirement and specify that the blocking for commonly used passwords or equivalent must be implemented for "*all* accounts." [500.7(b)(2)]

The Proposed Amendments also change some of the pre-proposal requirements for vulnerability management and access control programs, including:

- Removing the pre-proposal requirement for weekly scans and instead requiring Covered Entities to have a "**monitoring process** in place to ensure they are *promptly informed* of the emergence of new security vulnerabilities." [500.5(b)]\

- Adding a requirement for **timely remediation**, prioritized based on risk. [500.5(c)]

- Replacing the pre-proposal obligation for Class A companies to have "password vaulting" for privileged accounts, with a requirement to have a **privileged access management solution** and an automated method of blocking commonly used passwords, or reasonable equivalent approved by the CISO. [500.7(b)(1)]

Clarifications on the Applicability of the Multi-factor Authentication (“MFA”) Requirements

The pre-proposal appeared to create a broad and prescriptive new MFA requirement. The Proposed Amendments revise the pre-proposal changes to Section 500.12 to provide that MFA is required for:

- Remote access to the covered entity’s information systems;
- Remote access to third-party applications, including cloud-based ones, from which nonpublic information is accessible; and
- *All* privileged accounts (removing the pre-proposal carve-out for service accounts).

Critically, the Proposed Amendments bring back the ability of the CISO to approve compensating controls for MFA, making this requirement less prescriptive.

Additional Requirements for Incident Notification

The Proposed Amendments also add the following provisions regarding incident reporting:

- **90-day response period for investigative findings** – Each covered entity is now required to provide NYDFS with requested information regarding the investigation of a notified cybersecurity event, in a standard electronic form. [500.17(a)(2)]
- **72-hours for third-party incidents –** Covered Entities are now required to report third-party cybersecurity incidents on a 72-hour notification deadline, starting from the time the Covered Entity becomes aware of the event. [500.17(a)(3)]

Deadlines for Compliance

The Proposed Amendments also extend the deadlines for compliance that were provided in the pre-proposal draft.

Unless specified below, Covered Entities will have to comply with these new requirements starting 180 days from the date that the Proposed Amendments become effective (which will be sometime after the close of the comment period on January 9, 2023, so no earlier than July 8, 2023).

- **Incident Notification** – 30 days from the effective date. [500.17]
- **Backups** – One year from the effective date. [500.16(e)]
- **Various Technical Controls –** 18 months from the effective date, including:
  - **Vulnerability Scans** [500.5(a)(2)]
  - **Password Policy** [500.07(b)]
  - **MFA** [500.12(b)]
  - **Web and Email Filtering** [500.14(a)(2)]
  - **Endpoint Detection and Logging** [500.14(b)]
- **Asset Inventory** – Two years from the effective date. [500.13(a)]

The authors would like to thank Debevoise Law Clerks Camilla Isern and Ned Terrace for their contribution to this blog post.

To subscribe to the Data Blog, please click here.

* * *

Please do not hesitate to contact us with any questions.

NEW YORK

Avi Gesser
agesser@debevoise.com

Erez Liebermann
eliebermann@debevoise.com

Caroline N. Swett
cnswett@debevoise.com

Johanna N. Skrzypczyk
jnskrzypczyk@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com

SANFRANCISCO

Mengyi Xu
mxu@debevoise.com