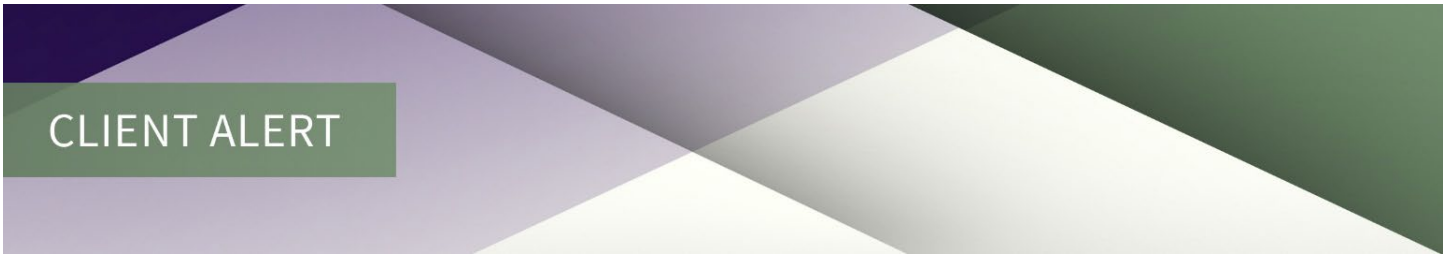

NYDFS Proposes Revisions to Second Set of Amendments to the Cybersecurity Regulation

July 10, 2023

AUTHORS

Daniel K. Alvarez | Kara Baysinger | Matthew J. Gaul | Laura Jehl
Allison J. Tam | Amelia Putnam

On June 28, 2023, the New York Department of Financial Services ("NYDFS") released further revisions to its proposed amendments (the "Revised Proposed Amendments") to 23 NYCRR Part 500 (the "Cybersecurity Regulation"), originally released on July 29, 2022.[1] We summarized the significant compliance requirements included in NYDFS's prior versions of its proposed amendments in Client Alerts here and here. In this latest set of revisions, NYDFS addressed several issues noted in comments submitted on the initial proposed amendments, incorporating certain suggestions and rejecting others.[2]

The practical result of the Revised Proposed Amendments is a proposal that includes significant additional details and requirements that would modify or further complicate covered entities' compliance obligations. In this Client Alert, we highlight some of those new proposed requirements and how NYDFS's revisions relate to the record of comments already submitted. Covered entities subject to the Cybersecurity Regulation will need to carefully review the Revised Proposed Amendments and consider whether to comment. The comment period for the Revised Proposed Amendments ends on August 14, 2023.

[1] New York State Department of Financial Services Revised Proposed Second Amendment to 23 NYCRR 500, Cybersecurity Requirements for Financial Services Companies, located here: https://www.dfs.ny.gov/system/files/documents/2023/06/rev_rp_23a2_text_20230628.pdf.

[2] Assessment of Public Comments on the Proposed Second Amendment to 23 NYCRR 500, located here: https://www.dfs.ny.gov/system/files/documents/2023/06/rev_rp_23a2_apc_20230628.pdf ("Assessment").

Overview of Changes

The Revised Proposed Amendments modify certain elements of the proposed amendments in significant ways. Specifically:

- New Defined Terms. The Revised Proposed Amendments would add several new defined terms, including Chief Information Security Officer or CISO, Independent Audit, Privileged Account, and Senior Governing Body.[3] NYDFS partially agreed with public comments concerning certain definitions. For example, NYDFS agreed that it would be appropriate to include internal auditors within the definition of "independent audit," but rejected suggestions to add additional parameters around independent audits because such limitations may not be appropriate for all covered entities.[4]

- Internal Cybersecurity Reporting. The CISO would need to annually report to the senior governing body about the covered entity's cybersecurity program and other information, such as plans for remediating material inadequacies, significant updates to the covered entity's risk assessment, and significant cybersecurity events.[5] NYDFS agreed with public comments that only significant updates to the risk assessment or significant cybersecurity events should be reported to the senior governing body, and revised the language of its proposal to limit such reporting to significant events.[6]

- Additional Requirements for the Senior Governing Body. The Revised Proposed Amendments would require the senior governing body to (i) exercise effective oversight of the covered entity's cybersecurity risk management; (ii) have sufficient understanding of cybersecurity-related matters to exercise such oversight; and (iii) require the covered entity's executive management to develop, implement, and maintain the covered entity's cybersecurity program.[7] NYDFS rejected comments that requested that a senior officer, rather than the senior governing body, review and approve cybersecurity policies, concluding that "[h]aving the senior governing body approve the policy is the most effective way to achieve [sufficient oversight], as opposed to relying on an intermediary to directly or indirectly approve and relay that information to the board or other senior governing body."[8]

- Access Privileges. Among other new requirements for access controls and privileges, a covered entity's cybersecurity program would be required to limit (i) user access privileges to information systems to those necessary to perform the user's job, (ii) the number of privileged accounts and the access functions of such privileged accounts to only those necessary to perform the user's job, and (iii) the use of privileged accounts to only

3 Revised Proposed Amendments, Section 500.1(c), (g), (m), and (p).
4 Assessment, at 15.
5 Revised Proposed Amendments, Section 500.4(b) and (c).
6 Assessment, at 31–32.
7 Revised Proposed Amendments, Section 500.4(d).
8 Assessment, at 22.

when performing functions requiring the use of such access.[9] NYDFS declined suggestions from public comments to add a safe harbor with respect to the access privileges.[10] NYDFS also explained that user access privilege review is "a risk mitigation tool that businesses of all sizes should utilize as a basic cyber hygiene measure."[11]

- Asset Inventory. A covered entity would be required to implement written policies and procedures designed to ensure a complete and documented asset inventory of the covered entity's information systems. This would need to include a method to track key information for each asset (e.g., owner, location, classification or sensitivity) and the frequency required to update and validate the covered entity's asset inventory.[12] Some public comments argued that maintaining an asset inventory would be too burdensome because of the additional work and details required given the prescriptive requirements in the proposed amendments, but NYDFS responded that maintaining an asset inventory is a "critical part of identifying assets that need to be protected" and noted that NYDFS provides a free asset inventory on its website for small- and medium-sized companies.[13]

- Business Continuity and Disaster Recovery Plans. The Revised Proposed Amendments would require covered entities to develop and implement business continuity and disaster recovery plans for their information systems and material services.[14] As part of that requirement, the Revised Proposed Amendments would add to the other testing requirements proposed in previous amendments a new requirement that a covered entity annually tests its ability to restore its critical data and information systems from backups.[15] Covered entities' incident response plans would also need to include procedures to prepare a root cause analysis that describes how the security event occurred, what business impact it had, and what will be done to prevent reoccurrences.[16] Public comments pointed out the significance of conducting a post-mortem after an incident occurs to improve a covered entity's cybersecurity program and determine the root cause of an incident. NYDFS agreed with these public comments and added the requirement that covered entities must include processes to prepare a root cause analysis in their incident response plans.[17]

- Reporting Requirements. The Revised Proposed Amendments would add requirements for covered entities to report to the NYDFS superintendent cybersecurity events that impact privileged accounts and cybersecurity events that resulted in the deployment of ransomware in a material part of the covered entity's information systems.[18] The

9 Revised Proposed Amendments, Section 500.7(a).
10 Assessment, at 7.
11 *Id.* at 46.
12 Revised Proposed Amendments, Section 500.13(a).
13 Assessment, at 61–62.
14 Revised Proposed Amendments, Section 500.16(a)(2).
15 Revised Proposed Amendments, Section 500.16(d).
16 Revised Proposed Amendments, Section 500.16 (b)(7)(ix).
17 Assessment, at 70–71.
18 Revised Proposed Amendments, Section 500.16(a)(1).

Revised Proposed Amendments replace a proposal that would have required covered entities to provide additional information to the NYDFS superintendent within 90 days of a request for additional information with a new, more demanding proposal that would require covered entities to *promptly* provide any requested information and would impose an express continuing obligation to update and supplement the information provided.[19] NYDFS explained that these revisions were made in response to public comments that explained the difficulty of complying with the proposed 90-day timeframe.[20]

- Annual Certification and Recordkeeping. The Revised Proposed Amendments proposes to replace the strict annual certification requirement with a more reasonable requirement that covered entities would be required to certify that they *materially* complied with the Cybersecurity Regulation during the prior calendar year.[21] Public comments requested that the annual certification requirement should allow for a form of material compliance, and NYDFS accepted that proposal in the Revised Proposed Amendments.[22]

- Violations. The Revised Proposed Amendments clarify that a *material* failure of a covered entity to comply with any part of the Cybersecurity Regulation for any 24-hour period would be a violation of the Cybersecurity Regulation.[23] When assessing penalties, the Revised Proposed Amendments would require the NYDFS superintendent to consider various factors, including the extent to which the covered entity's policies and procedures comply with nationally recognized cybersecurity frameworks, such as those from the National Institute of Standards and Technology ("NIST").[24] NYDFS agreed with public comments that failures with the Cybersecurity Rule for a 24-hour period should be material, but NYDFS rejected other scienter requirements because it noted that the assessment of penalties in § 500.20(c) includes a factor concerning the good faith of the covered entity.[25]

- Compliance Periods. The Revised Proposed Amendments include updated compliance deadlines for certain requirements, including the requirements concerning CISOs and senior governing bodies as well as the implementation of encryption policies (one year from the effective date of the Revised Proposed Amendments), and the requirements concerning the use of multifactor authentication (two years from the effective date of the Revised Proposed Amendments).[26] NYDFS rejected most suggestions from public comments that the effective date of the

19 Revised Proposed Amendments, Section 500.17(a)(2).
20 Assessment, at 81.
21 Revised Proposed Amendments, Section 50017(b).
22 Assessment, at 82.
23 Revised Proposed Amendments, Section 500.20(b).
24 Revised Proposed Amendments, Section 500.20(c).
25 Assessment, at 88–89.
26 Revised Proposed Amendments, Section 500.22(d).

amendments should be delayed, but NYDFS did increase the compliance period for certain requirements as described previously.[27]

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Daniel K. Alvarez
202 303 1125
dalvarez@willkie.com

Kara Baysinger
415 858 7425
kbaysinger@willkie.com

Matthew J. Gaul
212 728 8261
mgaul@willkie.com

Laura E. Jehl
202 303 1056
ljehl@willkie.com

Allison J. Tam
212 728 8282
atam@willkie.com

Amelia Putnam
202 303 1089
aputnam@willkie.com

[27] Assessment, at 89–92.