WILLKIE FARR & GALLAGHER LLP

CLIENT ALERT

NYDFS Proposes Significant Amendments to its Cybersecurity Regulation; Leading to Increased Compliance Obligations for Covered Entities

August 29, 2022

AUTHORS

Laura E. Jehl | Kara Baysinger | Matthew J. Gaul | Allison J. Tam
Michelle Bae | Kari Prochaska

On July 29, 2022, the New York Department of Financial Services ("NYDFS") released pre-proposal amendments[1] (the "Proposed Amendments") to its 23 NYCRR Part 500 (the "Cybersecurity Regulation"), which would bring significant changes and impose new requirements on covered entities. Among other things, the Proposed Amendments would add a new 24-hour notice requirement for any cybersecurity event where an extortion payment has been made, heighten oversight responsibilities of the board of directors and senior management, and create additional cybersecurity requirements for large covered entities by establishing a new class of covered entities called "Class A companies." If the Proposed Amendments are adopted, covered entities subject to the Cybersecurity Regulation would be required to review their existing policies and procedures and potentially make substantial changes to their cybersecurity programs.

Implications and Takeaways

Highlighted below are the key takeaways and implications for covered entities, if the Proposed Amendments are adopted.

[1] Proposed Second Amendment to 23 NYCRR 500, available at https://www.dfs.ny.gov/system/files/documents/2022/07/pre_proposed_draft_23nycrr500_amd2.pdf.

- ***NYDFS's ongoing focus on ransomware***. The Proposed Amendments signal a continued focus on ransomware incidents by the NYDFS.[2] Generally, many covered entities have been reporting ransomware incidents to the NYDFS under the current Cybersecurity Regulation, since most incidents have a reasonable likelihood of materially harming a material part of normal operations or require notification to other regulatory entities. Under the Proposed Amendments, a covered entity would be required to report to the NYDFS, in its normal course, any ransomware that is deployed within a material part of the covered entity's information system. Further, a covered entity's incident response plan would need to include a notification trigger if a single privileged account is accessed, even if the privileged access is discovered and remediated before any damage to a covered entity's systems occurs.

- ***Increased senior management and CISO responsibilities***. Covered entities would be required to alter organizational structures and responsibilities to give the CISO authority to make binding decisions regarding the cybersecurity program. The Proposed Amendments do not define what constitutes "adequate independence," although the closest analog may be the internal audit function, which generally reports directly to the audit committee of the Board of Directors. In addition, in order to show adequate independence from the information technology team, covered entities should consider whether the CIO/CTO/IT Manager and CISO should report separately to senior officer(s).

  Additionally, the CISO should no longer "consider," but must "address" the listed items in the report to the senior governing body. A covered entity's CISO should be prepared to report more frequently to the senior governing body regarding major updates such as risk assessment and major cyber events. It is assumed that "major cyber events" would include trends in cyberattacks, and the CISO may want to consider engaging cybersecurity counsel and consultants for assistance in determining what meets the definition of "major cyber events" at any given time. In addition to identifying vulnerabilities, covered entities must demonstrate the extra compliance step of drafting documented remediation plans that will be shared with the senior governing body.

- ***Review existing cybersecurity program***. Given the number of specific requirements that would be required to be addressed with respect to a covered entity's cybersecurity program, covered entities would need to conduct an extensive review of their existing cybersecurity policies and procedures and implement enhanced cybersecurity controls. For instance, while covered entities were previously required to have asset inventory and device management policies and procedures, the Proposed Amendments significantly expand what must be included in these policies and procedures, which may present a compliance burden for some covered entities. Additionally, although covered entities may be already encrypting data both in transit and at rest as a best practice, such practice must be documented in policies and procedures under the Proposed Amendments.

[2] *See* Ransomware Guidance (June 30, 2021), New York State Department of Financial Services, available at https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210630_ransomware_guidance.

- ***Additional compliance costs for covered entities***. All covered entities would likely need additional resources to implement the changes that are required by the Proposed Amendments. For example, to come into compliance with the new "operational resilience" requirements, covered entities would need to implement and test backups and business continuity and disaster recovery plans. Smaller covered entities may not have previously engaged in such extensive review and documentation. Covered entities with sophisticated cybersecurity programs may also experience an increase in cybersecurity costs. For instance, covered entities that meet the threshold of a Class A company would be required to engage an external third-party service provider to perform an updated risk assessment—regardless of the results of the previous risk assessment—at least once in three years. Annually, Class A companies would need to schedule and retain a third-party service provider to conduct an independent audit of their cybersecurity programs, which will likely be a Systems and Organizational Controls ("SOC") 2, Type 2 audit and may take a year or more to schedule and complete. For other cybersecurity controls, such as scanning, endpoint management and response, and privileged access monitoring, covered entities may need to purchase these technologies or utilize a managed security services provider.

- ***Changes to the Annual Reporting to the NYDFS***. In light of the new option to submit a written acknowledgement of noncompliance, the Proposed Amendments provide a roadmap for covered entities that are not in compliance to have a clearer avenue to identify areas of noncompliance to the NYDFS, so that they are not required to either falsely certify, or forego the certification process entirely. The practical impact on covered entities would be an increased volume of required documentation and record-keeping to monitor both present- and prior-year compliance, which may include filing more detailed paperwork evidencing the relevant compliance determination. Documentation would be required to identify where a covered entity is noncompliant, and include prospective remediation schedules.

- ***Other compliance challenges***. For certain covered entities, it may be likely that 180 days is not enough time to comply with several of the new, prescriptive requirements, particularly with respect to the more technical requirements. For example, the requirement for a Class A company to obtain a third-party audit may not be achievable within 180 days, regardless of the internal resources deployed. In addition, the transition times for compliance with amendments are potentially too onerous for many covered entities, particularly with respect to the 30-day window for compliance with the certification requirements under Section 500.17.

Summary of the Key Proposed Amendments

New Notification and Certification Requirements

- *Notification of cybersecurity events*. Covered entities are currently required to notify the NYDFS within 72 hours of a cybersecurity event if that event requires notification of any other governmental body, self-regulatory agency or any supervisory body, or if the cybersecurity event has a reasonable likelihood of materially harming any material part of the normal operation of the covered entity. The Proposed Amendments add two scenarios that

would also trigger the 72-hour notification requirement: a cybersecurity event where (i) an unauthorized user has gained access to a privileged account, or (ii) ransomware is deployed within a material part of the covered entity's information system.[3]

- *24-hour notification requirement when an extortion payment has been made.* The Proposed Amendments also add a completely new requirement that a covered entity that makes an extortion payment in connection with a cybersecurity event to notify the NYDFS within 24 hours. In addition, a written description detailing specific information related to the payment must be submitted to the NYDFS within 30 days of the extortion payment.[4]

- *Annual certification*. In connection with a covered entity's annual certification of compliance, the Proposed Amendments require that such certification must be signed by two specified officers of the covered entity, the CEO and Chief Information Security Officer ("CISO").[5] Under the current Cybersecurity Regulation, a covered entity has an option to submit the annual certification by its highest governing body (e.g., board of directors) or senior officer(s) responsible for the covered entity's management, operations, security, information systems, compliance and/or risk. Further, the Proposed Amendments require that the annual certification must be based on sufficient data and documentation to demonstrate full compliance.[6]

  The Proposed Amendments close a gap in the existing Cybersecurity Regulation by allowing a covered entity to choose to alternatively provide written acknowledgement that the covered entity did not fully comply with the Cybersecurity Regulation by describing the areas of noncompliance, including systems and processes that require material improvement, updating, or redesign and a remedial plan.[7] Similar to the annual certification requirement, covered entities must maintain all records and documentation relating to the acknowledgement of noncompliance, including the remedial plans and a timeline for implementation of remedial efforts.

Governance and Oversight

The Proposed Amendments would require increased oversight by a covered entity's "senior governing body," which means a covered entity's board of directors (or an appropriate committee thereof) or equivalent body, or if neither exists, the senior officer of the covered entity responsible for the covered entity's cybersecurity program. The senior governing body is tasked with approving the covered entity's written policies at least annually. If the covered entity has a board of directors, the Proposed Amendments require that the board or an appropriate committee of the board must have sufficient

3 Section 500.17(a)(3)-(4)
4 Section 500.17(c)
5 Section 500.17(b)(2)
6 Section 500.17(b)(1)(i)(b)
7 Section 500.17(b)(1)(ii)

expertise and knowledge to exercise effective oversight of cyber risk.[8] The board must require the covered entity's executive management or its delegates to develop, implement, and maintain the information security program.[9] With respect to any penetration testing conducted, a covered entity must ensure that any material gaps found are documented and reported to the senior governing body and senior management.[10] As explained above, the covered entity's CEO must sign the annual certification of compliance, together with the CISO (or by the senior officer responsible for the covered entity's cybersecurity program if the covered entity does not have a CISO).

A covered entity's CISO would also have additional responsibilities under the Proposed Amendments. The CISO must timely report to the senior governing body regarding material cybersecurity issues, such as updates to the covered entity's risk assessment or major cyber events.[11] In an annual report to the senior governing body, the CISO must address any plans for remediating inadequacies identified in the covered entity's cybersecurity program.[12] The Proposed Amendments require that the CISO be given adequate independence and authority to ensure cybersecurity risks are appropriately managed.[13]

Cybersecurity Policies and Procedures

The Proposed Amendments set forth additional areas that must be covered in written policies and procedures:

- the minimum topics that must be addressed in cybersecurity policies and procedures, if determined to be necessary based on the covered entity's risk assessment, including the additions of end-of-life management, remote access, and vulnerability and patch management;[14]
- enhanced policies and procedures regarding asset inventory, which must be designed to ensure a complete, accurate, and documented asset inventory, including all information systems and their components such as hardware;[15]
- a new written policy requiring encryption over external networks and at rest;[16]

8 Section 500.4(d)
9 *Id*.
10 Section 500.5(b)
11 Section 500.4(c)
12 Section 500.4(b)
13 Section 500.4(a)
14 Section 500.3(c), (d), (o)
15 Section 500.13
16 Section 500.15(a)

- significantly enhanced policies and procedures on operational resilience, including a new requirement that covered entities implement business continuity and disaster recovery plans in addition to their incident response plan, which must be periodically tested.

The Proposed Amendments further require that a covered entity's incident response, business continuity and disaster recovery plans be shared with relevant employees and that they receive training. The periodic testing of these plans must involve all staff critical to the response, including senior officers and the CEO.

Cybersecurity Controls and Measures

Covered entities would also be required to implement additional and enhanced cybersecurity controls under the Proposed Amendments:

- *Risk assessments and security assessments*
    - Risk assessments would be required to cover a broad set of topics that are not currently specified in the Cybersecurity Regulation.
    - Risk assessments would need to be updated at least annually and impact assessments must be conducted whenever a change in the business or technology causes a material change to the covered entity's cyber risk.
    - Penetration testing to be conducted by a qualified independent party would be required at least annually.
    - Vulnerability assessments would have to be conducted regularly; under the existing regulation, such assessments are required bi-annually.
- *Cybersecurity controls*
    - Access control requirements would be considerably enhanced, including requirements that all privileged accounts be periodically reviewed and that accounts and access that are no longer necessary be removed.
    - Multi-factor authentication ("MFA") would be required for remote access to network, enterprise, and third-party applications from which nonpublic information ("NPI") is accessible, as well as for privileged accounts, except service accounts that meet certain criteria and where the CISO has approved in writing the implementation of controls that achieve reasonably equivalent security.
    - Emails must be monitored and filtered to block malicious content.
    - Cybersecurity training would be required to cover phishing training, exercises, and simulations when appropriate.

Additional Cybersecurity Obligations on Large Covered Entities – "Class A Companies"

The Proposed Amendments would create a new category of larger companies, "Class A companies," which are covered entities that have (1) more than 2,000 employees, including the covered entity and all of its affiliates or (2) $1 billion in gross annual revenue averaged over the last three fiscal years from all business operations of the covered entity and all of its affiliates. In addition to the cybersecurity controls described above, Class A companies would be required to:

- at least annually, conduct an independent audit of their cybersecurity programs;[17]
- at least once every three years, use external experts to conduct a risk assessment;[18]
- at least weekly, conduct systematic scans or reviews as part of conducting vulnerability assessments;[19]
- monitor privileged access activity and implement a password vaulting solution for privileged accounts and an automated method of blocking commonly used passwords;[20]
- implement an endpoint detection and response solution to monitor anomalous activity and a solution that centralizes logging and security event alerting.[21] The covered entity's CISO may choose to implement reasonably equivalent or more secure access controls or endpoint detection, if such measures are approved in writing.

Exemption

The Proposed Amendments would expand the limited small company exemption to covered entities with fewer than 20 employees (it currently applies to covered entities with fewer than 10 employees) or covered entities with less than $15,000,000 in year-end total assets (it currently applies to entities with less than $10,000,000 in year-end total assets). The limited exemption continues to apply to certain provisions and not the Cybersecurity Regulation as a whole.

Violations and Penalties

Under the Proposed Amendments, committing a single act prohibited by the Cybersecurity Regulation or the failure to act to satisfy an obligation would constitute a violation. A failure to comply for any 24-hour period with any section or subsection of the Cybersecurity Regulation or a failure to secure or prevent unauthorized access to NPI due to noncompliance would be considered a violation. The Proposed Amendments list the mitigating factors that the NYDFS would be permitted to consider when assessing penalties for a violation.

---

17 Section 500.2(c)
18 Section 500.9(d)
19 Section 500.5(a)(2)
20 Section 500.7(b)
21 Section 500.14(b)

If the Proposed Amendments are adopted, any data security incident that allows access to or fails to secure NPI, or any act of noncompliance with any part of the Cybersecurity Regulation for a 24-hour period, would be considered a violation of the Cybersecurity Regulation as a whole. For example, if the entity's CISO resigned and was not replaced within 24 hours, a violation would occur. Similarly, a covered entity might not realize that it was out of compliance within that 24-hour window, thus triggering a violation. If this language is codified, it will place a significant burden on any covered entity that cannot remediate a deficiency within 24 hours. Although this appears to be a more stringent requirement in terms of the regulatory language, it is consistent with NYDFS enforcement of the Cybersecurity Regulation to date.

Effective Dates

The Proposed Amendments would take effect 180 days from the date they are adopted, except the notice requirements and annual certification or acknowledgement requirement, which would take effect 30 days after adoption, and certain requirements such as MFA, endpoint detection requirements for Class A companies, which would take effect one year after adoption.

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

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

Kara Baysinger
415 858 7425
kbaysinger@willkie.com

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

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

Michelle Bae
202 303 1166
ebae@willkie.com

Kari Prochaska
312 728 9080
kprochaska@willkie.com