Articles + Publications | December 13, 2022

New York DFS Cybersecurity Regulation Update: ?Amendments Proposed November 2022

Privacy & Cybersecurity Newsletter

WRITTEN BY

Theodore P. Augustinos | Alexander R. Cox

Licensees of the New York Department of Financial Services ("DFS") should be tracking the proposed amendments to the DFS Cybersecurity Regulation. All covered entities under the Regulation will need to revisit their cybersecurity preparedness to satisfy the enhanced regulatory requirements, particularly large entities that meet the definition of "Class A companies" introduced by the proposed amendments. Importantly for many covered entities, the limited exemption for small entities will be expanded to include more entities, and the threshold based on number of employees and independent contractors will be clarified.

Timing

The DFS Cybersecurity Regulation became effective March 1, 2017, with transition periods for various requirements for the next two years. The currently proposed amendments were published November 9, 2022, with the comment period expiring January 9, 2023. Once finalized, the proposed amendments will become effective sometime after the comment period ends, upon publication in the State Register.

Implications for Large Entities

The proposed amendments add the term Class A company to mean:

covered entities with at least $20,000,000 in gross annual revenue in each of the last two fiscal years from business operations of the covered entity and its affiliates in [New York] and:

(1) over 2,000 employees averaged over the last two fiscal years, including those of both the covered entity and all of its affiliates no matter where located; or

(2) over $1,000,000,000 in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and all of its affiliates.

Class A entities will be subject to the following new or enhanced requirements under the proposed amendments:

i. Annual Cybersecurity Program Audit. The cybersecurity program required under Section 500.2 must be independently audited at least annually.
ii. Privilege Access Activity Monitoring. In addition to enhanced safeguards for access privileges under Section

500.7 introduced for covered entities generally (as described below), Class A companies will also be required to monitor privileged access activity, and to implement (a) a privileged access solution, and (b) an automated method of blocking commonly used passwords.

iii. Risk Assessments. In conducting the periodic risk assessment required by Section 500.9, Class A companies must use external experts.

iv. Enhanced Monitoring. For Class A companies, the monitoring requirements of Section 500.14 are enhanced to require (a) endpoint detection and response solutions, and (b) centralized logging and security event alerting. The CISO can approve the use of reasonably equivalent or more secure controls or tools.

Changes to the Limited Exemption for Small Entities

Fortunately for many small businesses, the proposed amendments increase the thresholds for certain covered entities to qualify for the limited exemption under Section 500.19(a). If the covered entity meets any one of three different thresholds, based on (i) headcount, (ii) revenue, or (iii) assets, the limited exemption will apply. The thresholds based on the number of employees and independent contractors of the covered entity and its affiliates is increased from 10 to 20; the threshold based on total assets is increased from $10 million to $15 million.

For purposes of counting the employees and independent contractors of the covered entity and its affiliates toward the threshold, the DFS Cybersecurity Regulation currently includes only employees and independent contractors "located in New York or responsible for business of the covered entity." Unfortunately, the proposed amendments delete this important qualifier, and therefore count all such persons, regardless of location or responsibility.

As a result, more small entities will qualify for the limited exemption, except that more small entities with one or more affiliates will now exceed the threshold based the number of employees and independent contractors.

There is also a threshold for covered entities with less than $5 million in gross annual revenue. The proposed amendments limit the revenue counted toward this threshold by adding "in this State," thereby making the limited exemption available to more covered entities.

The proposed changes to the limited exemption for small entities can be expected to exempt more covered entities from the full menu of requirements imposed by the DFS Cybersecurity Regulation. It should be emphasized, however, that the limited exemption is limited to many, but not all of the requirements for administrative and technical safeguards; small entities subject to the limited exemption will continue to be subject to many of the requirements of the DFS Cybersecurity Regulation.

The proposed amendments exclude the requirement for multi-factor authentication under Section 500.12 from the limited exemption. Therefore, covered entities to which the limited exemption applies, as well as covered entities exempted by the proposed amendments, would be subject to this requirement.

Changes of General Applicability

The proposed amendments include many clarifications, enhancements and other changes that would not impose substantive new requirements, but there are also many changes that may require advance planning by most covered entities.

1. *Cybersecurity Policy Annual Approval Requirement.* The proposed amendments require approval of a

cybersecurity policy required by Section 500.3 by the senior governing body of the covered entity, not by a senior officer or the board of directors, at least annually.

2. *CISO Requirements.* Under the proposed amendments to Section 500.4, the CISO "must have adequate authority to ensure cybersecurity risks are appropriately managed, including the ability to direct sufficient resources to implement and maintain a cybersecurity program. There is also a new requirement to report material cybersecurity issues to the senior governing body. The board must also exercise appropriate cybersecurity oversight, and have or engage sufficient expertise and knowledge to do so.
3. *Written Policy for Vulnerability Management.* The proposed amendments require a specific written policy (or policies and procedures), adding specificity for the penetration testing requirement, and requiring automated scans (with manual scans for systems not covered by automated scans) to review vulnerabilities under Section 500.5.
4. *Enhanced Access Privilege Management.* Section 500.7 requires new limitations on the number and use of privileged accounts, a new defined term under the proposed amendments. Password management will require a written policy, and additional requirements are imposed on Class A companies, as noted above.
5. *Annual Requirement for Application Security Review.* Under the proposed amendments, the CISO must review the required procedures, guidelines and standards for developing, assessing, or testing applications used by the covered entity at least annually.
6. *Risk Assessment Review.* The proposed amendments require review and update of the risk assessment under Section 500.9 at least annually and whenever a change in the business or technology causes a material change to the covered entity's cyber risk.As noted above, Class A companies must use external experts to conduct the risk assessment at least every three years.
7. *Third Party Service Provider Policy Exception Deleted.* The limited exception for agents, employees, representatives and designees of covered entities from the Section 500.11 requirement for a third party service provider cyber risk management policy is deleted by the proposed amendments. It appears that this deletion was to eliminate a redundancy with the exemption of 500.19(b), which permits such covered entities to rely on a controlling covered entity's "cybersecurity program to the extent that the employee, agent, representative or designee is covered by the ?cybersecurity program of the covered entity?."
8. *Data Retention Requirements Expanded to Assess Management.* The proposed amendments substantially expand Section 500.13 beyond data retention to require "written policies and procedures designed to ensure a complete accurate and documented asset inventory" containing specified content.
9. *Expanded Monitoring Requirements.* Section 500.14 sets forth monitoring and training requirements, which the proposed amendments expand to require controls to protect against malicious code, including monitoring and filtering web traffic and electronic mail to block malicious content. Cybersecurity awareness training must be at least annual, and include social engineering exercises. Additional requirements for endpoint detection and response, centralized logging, and security event alerting, are requirements for Class A companies, as noted above.
10. *Business Continuity.* The incident response provisions of Section 500.16 are expanded by the proposed amendments to include business continuity plans "to investigate and mitigate disrupted events and ensure operational resilience, including but not limited to incident response, business continuity and disaster recovery plans," satisfying detailed requirements. There is a specific requirement to maintain secure backups.
11. *Notice of Cybersecurity Event, and Compliance Certificate.* The forms for required filings appearing as Appendices to the DFS Cybersecurity Regulation are removed by the proposed amendments, and replaced by forms to be posted on the DFS website. The annual compliance certificate required by Section 500.17 changes from a check box certification that the compliance requirements are satisfied to a more involved filing that would indicate any exceptions from full compliance, and provide a timeline to full compliance.

Under the proposed amendments, the required notice of a cybersecurity event must provide specific information where the event involved privileged accounts or ransomware, or any extortion payment. Notice of an extortion payment must be provided within 24 hours, and additional descriptions of the rationale and reasoning for the payment must be disclosed within 30 days. Information concerning the investigation of a cybersecurity event must be provided within 90 days. The proposed amendments also formalize the previously

stated DFS position that covered entities must file notices of cybersecurity events directly, and cannot have service providers file on their behalf.

12. *Enforcement.* The proposed regulations provide additional guidance concerning enforcement by the superintendent pursuant to Section 500.20.
13. *Effective Date.* The proposed regulations will become effective pursuant to Section 500.22 upon publication, and covered entities will have 180 days to comply, except for transitional periods of 30 days for the compliance certificate and notice of cybersecurity event provisions of Section 500.17; one year for the requirements under Section 50.16(e) and 500.19(a), which address backups and the limited exemption, respectively; and 18 months for the requirements of:

    - Section 500.5(a)(2) (automated scans);
    - Section 500.7(b) (password policy, and Class A company requirements to monitor privileged access);
    - Section 500.12(b) (enhanced multi-factor authentication requirements);
    - Section 500.14(a)(2) (protections against malicious code); and
    - Section 500.14(b) (Class A company requirements for endpoint detection, and centralized logging and security event alerting).
14. *Exemptions from Electronic Filing.* New Section 500.24 added by the proposed amendments permit covered entities to apply for an exemption from the requirement to submit filings online.

All covered entities will be affected by the proposed amendments to the DFS Cybersecurity Regulation, and will require significant expenditure of resources to comply with new or expanded requirements, and some may be newly eligible for the limited exemptions.

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber