Cullen | Dykman

New York State Department of Financial Services Proposes Amendments to Cybersecurity Regulation

December 15, 2022

The New York Department of Financial Services ("DFS") has released proposed amendments ("Proposed Amendments") to its Cybersecurity Regulation, Part 500 of Title 23 of the New York Codes, Rules, and Regulations ("Part 500"). The Proposed Amendments would substantially expand the scope of Part 500 by, among other things, broadening senior management's governance and oversight responsibilities, designating a class of entities subject to heightened requirements, mandating new reporting obligations for ransomware attacks and extortion payments, and expanding requirements for required contents in cybersecurity policies and procedures.

Background

Part 500, which has been in effect since March 2019, requires covered entities[1] to maintain a comprehensive cybersecurity program in accordance with several specific security requirements.

While most of the Proposed Amendments would take effect 180 days from the date of adoption, certain provisions would take effect at various points over the next two years. Comments on the Proposed Amendments are due by January 9, 2023.

The Proposed Amendments

New Incident Reporting Requirements

Covered entities are already required to notify DFS within **72 hours** of certain cybersecurity events. The Proposed Amendments would require notification to DFS in the event of:

- Any cybersecurity event that has a reasonable likelihood of materially disrupting or degrading any material part of the covered entity's normal operations;
- Any unauthorized access to a privileged account or deployment of ransomware within a material part of the covered entity's information system;
- Any cybersecurity event at a third party service provider that affects a covered entity; and
- An extortion payment made in connection with a cybersecurity event involving the covered entity (such notice to be made within 24 hours).

Additionally, within 30 days of an extortion payment, a covered entity would be required to provide DFS with a written description of the reasons payment was necessary, a description of alternatives to payments considered, all diligence performed to find alternatives to payment, and all diligence performed to ensure compliance with applicable rules and regulations.

Annual Reporting and Certifications

Part 500 presently requires covered entities to submit annual certifications of compliance to DFS. The Proposed Amendments would require the covered entity's highest-ranking executive and Chief Information Security Officer ("CISO") to annually sign the certification of compliance or, alternatively, a document acknowledging that the covered entity did not fully comply with all the requirements of Part 500. Such acknowledgment would need to provide remediation plans and a timeline for their implementation and identify all sections of Part 500 with which the entity did not fully comply, along with the nature and extent of such noncompliance.

Additional Board Governance and Oversight

Senior governing bodies, the CISO, and highest-ranking executive would be vested with broad governance and oversight duties under the Proposed Amendments. Such duties include:

- The senior governing body must approve the covered entity's written policies at least annually;
- The board or an appropriate committee thereof must exercise oversight of, and provide direction to management on, the covered entity's cybersecurity risk management and must have sufficient expertise and knowledge to exercise effective oversight;
- The CISO must timely report to the senior governing body regarding material cybersecurity issues; and
- Material issues found in penetration tests or vulnerability assessments must be documented and reported to the senior governing body and senior management.

Cybersecurity Policies and Procedures

A covered entity's policies and procedures would need to:

- Cover new topics that must be approved by the covered entity's governing body;
- Require a complete, accurate and documented asset inventory; and
- Require encryption that meets industry standards.

Incident Response

Part 500 currently requires covered entities to maintain an incident response plan. Under the Proposed Amendments, covered entities would be required to distribute their incident response plan to all necessary employees, train them on such plan, and test the plan annually.

The incident response plan would need to address different types of cybersecurity events, including disruptive events such as ransomware incidents.

Risk Assessments

The Proposed Amendments expand the definition of "risk assessment" to apply to the process of identifying cybersecurity risks to organizational operations, organizational assets, individuals, customers, consumers, other organizations, and critical infrastructure resulting from the operation of the information system. They elaborate on what such risk assessment must consider and specify that threat and vulnerability analyses must be incorporated. Risk assessments would need to be reviewed at least annually or whenever there was a change to a covered entity's business or technology that caused a material change to the entity's cybersecurity risk.

Business Continuity and Disaster Recovery ("BCDR")

The Proposed Amendments would add significant requirements for developing and maintaining a BCDR plan. A BCDR plan should identify critical systems, data, and operations, require routine backups, and include backup and recovery procedures in the event of a disaster, cyberattack, or other event. This plan must also be distributed to all necessary employees under the Proposed Amendments.

Vulnerability Management and Penetration Testing

The Proposed Amendments would broadly mandate that covered entities develop and implement written policies and procedures for vulnerability management, conduct annual internal and external penetration testing, and periodically conduct vulnerability scanning. Covered entities would have to have a monitoring process in place to ensure they are promptly informed of the emergence of new security vulnerabilities and remediate the risk posed.

Remote Access and Multi-Factor Authentication

The Proposed Amendments would require all remote access – both to the covered entity's systems and to third-party applications – to be secured with multi-factor authentication.

Class A Companies and Requirements

The Proposed Amendments would create a new category of "Class A" companies, which are defined as covered entities with at least $20,000,000 in gross annual revenue in each of the last two fiscal years and either more than 2,000 employees averaged over the last two fiscal years or averaged more than $1,000,000,000 in gross annual revenue in each of the last two fiscal years. Class A companies would be subject to additional requirements under Part 500.

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).

Violations

The Proposed Amendments would add specificity on what constitutes a Part 500 violation. A violation would be defined as committing a single act prohibited by Part 500 or the failure to act to satisfy an obligation. Acts or

failures would include, but not be limited to:

- The failure to secure or prevent unauthorized access to an individual's or an entity's nonpublic information due to noncompliance with any section of Part 500; or
- The failure to comply for any 24-hour period with any section or subsection of Part 500.

The Proposed Amendments also specify the factors that the DFS may consider when assessing penalties for violations, such as the extent to which the covered entity cooperated with DFS in its investigation, good faith of the covered entity, and whether the violations resulted from conduct that was unintentional or inadvertent, reckless, or intentional or deliberate.

Conclusion

The Proposed Amendments would significantly increase obligations for covered entities in the financial services industry under Part 500. Comments must be submitted in writing to DFS by 5 pm EST on Monday, January 9, 2023. Submissions should be sent by email to cyberamendment@dfs.ny.gov or by mail to the New York State Department of Financial Services c/o Cybersecurity Division, Attn: Joanne Berman, One State Street, Floor 19, New York, NY, 10004. No special form is required.

This advisory is a general overview of DFS's Proposed Amendments and is not intended as legal advice. The requirements under the Proposed Amendments of Part 500 are very detailed and must be reviewed in their totality.

If you have any questions about Part 500 or its Proposed Amendments, please feel free to contact Joseph D. Simon at (516) 357-3710 or via email at **jsimon@cullenllp.com**, Kevin Patterson at (516) 296-9196 or via email at **kpatterson@cullenllp.com**, Elizabeth A. Murphy at (516) 296-9154, or via email at **emurphy@cullenllp.com**, or Gabriela Morales at (516) 357-3850 or via email at **gmorales@cullenllp.com**.

Footnotes

[1] "Covered entity" means any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the New York Banking Law, the Insurance Law or the Financial Services Law, regardless of whether the covered entity is also regulated by other government agencies. 23 NYCRR 500.1(c).

Practices

- Banking and Financial Services
- Regulatory and Compliance

Attorneys

- Joseph D. Simon
- Kevin Patterson

- Elizabeth A. Murphy
- Gabriela Morales