Akin®

NYDFS Amended Cybersecurity Rules: Overview of Upcoming Deadlines

December 19, 2023

Reading Time : **9 min**

By: Natasha G. Kohne, Erica Holland-Nesfield, Joseph Hold

On November 1, 2023, the New York Department of Financial Services (NYDFS) announced the adoption of amendments to its Cybersecurity Regulation 23 NYCRR Part 500 ("Amended Cybersecurity Rules" or "Amended Rules"). NYDFS adopted changes following formal notice and comment on the proposed amendments released in June 2023 (please find our piece on the proposed amendments here). NYDFS also released an "Assessment of Public Comment" describing why it adopted or rejected certain comments, providing a helpful sight into the Department's approach to the Cybersecurity Regulation.

More Obligations for the Largest Companies

The Amended Rules create a new subcategory for large covered entities called "Class A companies." Class A companies are covered entities with at least $20 million in gross annual revenue from its business operations and its affiliates in New York in each of the last two years, and either: (i) over 2,000 employees, including employees of its affiliates, no matter where located; or (ii) $1 billion in gross annual revenue for each of the past two fiscal years from all business operations and its affiliates no matter where located.[1] These Class A companies will now face several new cybersecurity requirements, including:

- **Independent Audits**: Design and conduct audits based on its risk assessment.[2] An independent audit must be conducted by internal or external auditors free to make decisions not influenced by the Company[3];
- **Monitoring**. Establish an endpoint detection and response solution for monitoring anomalous activity, including lateral movement, and a solution that centralizes logging and security event alerting;[4]
- **Privileged Access Activity**. Implement a privileged access management solution along with an automated method of blocking commonly used passwords for all accounts on information systems owned or controlled by the Company (to the extent feasible).[5]

New Notification Requirements

The Amended Rules expand notifications requirements and add "cybersecurity incident" as a new defined term, to align with the terms used in other regulations. Under the original Cybersecurity Regulations, covered entities were required to notify NYDFS within 72 hours of any cybersecurity event that (1) had an impact on the covered

entity and notice was required to any government body, agency or other supervisory body or (2) had a reasonable likelihood of harming a material part of normal operations. The Amended Rules add:

- Ransomware deployed within a material part of the covered entity's information systems[6] as an additional trigger;
- Prompt updates to be made to the superintendent with any information requested regarding a reported incident, including providing any previously unavailable new information;[7]
- A new 24-hour notification requirement for extortion payments connected to a cybersecurity event, that also entails submitting a written description within 30 days describing why payment was necessary, alternatives considered, and sanctions diligence conducted.[8]

Additional Governance Provisions

Although the original Cybersecurity Regulations featured many governance requirements for cybersecurity policies, the Amended Rules introduce enhanced obligations:

- *Enhanced Reporting to the Board*: Additional reporting by the CISO on "plans for remediating material inadequacies" and requirement to "timely" report "material cybersecurity issues such as significant cybersecurity events or significant changes made to the cybersecurity program."[9]
- *Executive Annual Certifications*: The required annual certification of compliance must now be signed by the highest-ranking executive of the covered entity and its CISO, instead of the senior officer as was originally required.[10]
- *Certification of Compliance for Prior Year*: The covered entity must now certify that it "materially complied" with the Cybersecurity Rule requirements "during the prior calendar year" and must be based on data and documentation sufficient to accurately determine and demonstrate this material compliance.[11]
- *Acknowledgement of Noncompliance*: In the event the CISO and highest-ranking executive cannot certify compliance, the Amended Rules require written acknowledgement that: (i) the entity did not materially comply, (ii) identify the sections that the covered entity did not comply with while describing the nature and extent of the noncompliance, and (3) provide a remediation timeline or confirmation that remediation has been completed.[12]
- *Tabletop Testing*: New annual tests requirements of incident response and business continuity and disaster recovery (BCDR) plan with all critical staff and management. The Amended Rules also require annual tests of the covered entity's ability to restore its critical data and systems from backups.[13]

New Incident Response Requirements

Covered entities face some new requirements for their incident response plans under the Amended Rules. These incident response plans must be reasonably designed for prompt response to and recovery from any cybersecurity event that materially affects the confidentiality, integrity or availability of a covered entity's information systems or the continuing functionality of "any aspect of the covered entity's business or operations."[14] Covered entities' incident response plans must now address both recovery from backups and "root cause analysis" under the Amended Rules. Root cause analysis must describe the details of how and why

the event occurred, the business impact of the event and what will be done to prevent a repeat of the event.[15]

Business Continuity Plan Requirements

The Amended Rules add new obligations for covered entities regarding business continuity plans. The previously mentioned BCDR plans are now required for covered entities, to ensure covered entities' information systems and material services remain available and functional in the event of a cybersecurity disruption.

BCDR plans must:

1. Identify documents, data, facilities, infrastructure, services, personnel and competencies essential to the continued operations of the covered entity's business;
2. Identify supervisory personnel responsible for implementing the BCDR plan;
3. Have a plan to communicate with essential persons in the event of a cybersecurity-related disruption;
4. Include procedures for the timely recovery of critical data and information systems and to resume operations as soon as reasonably possible;
5. Include procedures for backing up information essential to the operations of the covered entity and storing such information off-site; and
6. Identify third parties that are necessary to the continued operations of the covered entity's information systems.[16]

Revamped Risk Assessments

The definition of "risk assessment" was expanded to cover "the process of identifying, estimating and prioritizing cybersecurity risks to organizational operations (including mission functions, image and reputation), organizational assets, individuals, customers, consumers, other organizations and critical infrastructure resulting from the operation of an information system. Risk assessments incorporate threat and vulnerability analyses and consider mitigations provided by security controls planned or in place."[17] Risk assessments are now required to be reviewed and updated at a minimum annually and whenever a material change in the business or technology causes a material change to the covered entity's cyber risk.[18]

More Access Controls & Technical Controls

The original Cybersecurity Regulations required covered entities to establish policies and procedures for periodically disposing of nonpublic information, as well as limiting access privileges for users on information systems that provide access to nonpublic information. The Amended Rules establish additional controls for user access and retention, as well as technical requirements, including:

- *Multifactor Authentication*: Multifactor authentication (MFA) is required for "any individual accessing any information system of a covered entity."[19] The Amended Rules removed "text message on a mobile phone" from the list of permitted MFA authentication factors.[20]
- *Defense Against Malicious Code*: Covered entities must enact risk-based controls to protect against malicious code, including monitoring controls and web traffic filtering.[21]

- *Mandatory Encryption*: The Amended Rules removed the option for covered entities to use "effective alternative compensating controls" instead of encryption for nonpublic information in transit over external networks.[22]
- *Vulnerability Assessments*: For managing vulnerabilities, the Amended Rules require (i) annual penetration testing by a qualified external party; (ii) automated scans of information systems and a manual review of systems not covered by such scans to discover, analyze and report vulnerabilities at a frequency determined by the risk assessment; (iii) prompt informing of the covered entity on new vulnerabilities and having a monitoring process and (iv) timely remediation of vulnerabilities with priority given based on the risk the pose.[23]
- *Asset Management & Data Retention*: The Amended Rules require covered entities to implement policies and procedures designed to maintain a complete and accurate asset inventory of their information systems. These policies must include a method to track key information for assets, such as owner, location and classification or sensitivity. The policies must also include the frequency required to update and validate the covered entity's asset inventory.[24]
- *Access Privileges and Management*: Under the Amended Rules, covered entities are required to (i) limit user access privileges to nonpublic information systems to only those necessary to perform the user's job; (ii) limit the number and use of privileged accounts and limit access functions; (iii) review all use access privileges at least annually; (iv) review all user access privileges and remove unnecessary access at least annually; (v) disable or securely configure protocols that permit remote control of devices and (vi) promptly terminate access following departures.[25] The Amended Rules have redefined "privileged account" as "any authorized user account or service account that can be used to perform security-relevant functions that ordinary users are not authorized to perform, including but not limited to the ability to add, change or remove other accounts, or make configuration changes to information systems."[26] The Amended Rules also require covered entities to implement a written password policy, to the extent passwords are employed, that meets industry standards.[27]

New Enforcement Provisions

Notably, under the Amended Rules, the commission of a single prohibited act, or the failure to satisfy an obligation, constitutes a violation. These failures can include:

1. Failure to prevent unauthorized access to nonpublic information due to noncompliance with any section; or
2. A material failure to comply for any 24-hour period with any section.[28]

The NYDFS also included a list of mitigating factors in the Amended Rules that it will consider when assessing penalties, including but not limited to:

- Cooperation during the investigation, good faith, history of prior violations,
- Whether the act was intentional, whether accurate and timely disclosures were made,
- The extent of harm to customers, gravity of the violation, number of violations,
- The participation of senior governing body, penalties imposed by other regulators.[29]

Please see the table below for a timeline of when new provisions of the Amended Cybersecurity Rules will become effective:

Timeline of NYDFS Amended Cyber Rules Requirements	
December 1, 2023	Notification obligations to NYDFS (500.17)
April 15, 2024	Certification requirements (500.17(b))
April 29, 2024	Risk assessment requirements (500.9) Cybersecurity policy requirements (500.3) Penetration testing and monitoring requirements (500.5(a)(1), (b), and (c)) Training requirements (500.14(a)(3)) For Class A companies, audit requirements (500.2(c))
November 1, 2024	CISO, management, and board governance requirements (500.4) Encryption requirements (500.15) Incident response and business continuity planning and testing requirements (500.16)
May 1, 2025	Scanning requirements (500.5(a)(2)) Access privilege and password requirements (500.7) Requirements for protection against malicious code (500.14(a)(2)) For Class A companies, requirements relating to privileged access management solutions and blocking of commonly used passwords (500.7) For Class A companies, requirements for endpoint detection and response solutions and centralized logging (500.14(a)(2) and (b))

November 1, 2025	MFA requirements (500.12) Asset inventory requirements (500.13(a))

To assist impacted businesses with keeping track of important compliance dates, NYDFS published Cybersecurity Implementation Timelines for small businesses, Class A businesses, and covered entities, and announced that it will host webinars to assist regulated entities with compliance.

Please contact a member of Akin's cybersecurity, privacy and data protection team if you have any questions about these amendments or how they will affect your company.

---

[1] 23 NYCRR § 500.1(d), when determining the number of employees and the gross annual revenue, the term "affiliates" should include "only those that share information systems, cybersecurity resources, or all or any part of a cybersecurity program with the covered entity."

[2] *Id*. at 500.2(c).

[3] *Id.* at 500.1(h).

[4] *Id*. at 500.14(b).

[5] *Id*. at 500.7(c) Alternatively, the covered entity's CISO may instead approve in writing at least annually the infeasibility and the use of reasonably equivalent or more secure compensating controls.

[6] *Id*. at 500.1(g).

[7] *Id*. at 500.17(a)(2).

[8] *Id*. at 500.17(c) this includes applicable rules from the Office of Foreign Assets Control (OFAC).

[9] *Id*. at 500.4(b), (c).

[10] *Id*. at 500.17(b).

[11] *Id*. at 500.17(b)(1) This can include documentation from officers, employees, representatives, outside vendors and other individuals or entities, as well as reports, certifications and schedules.

[12] *Id*. at 500.17(b)(1)(ii).

[13] *Id*. at 500.16(d).

[14] *Id*. at 500.16(a)(1).

[15] *Id*.

[16] *Id*. at 500.16(a)(2).

[17] *Id*. at 500.1(p).

[18] *Id*. at 500.9(a).

[19] *Id*. at 500.12(a), (b), there are limited exceptions to this requirement for small entities, and the CISO may approve use of reasonably equivalent or more secure compensating controls, to be reviewed annually at a minimum.

[20] *Id*. at 500.1(j).

[21] *Id*. at 500.14(a)(2).

[22] *Id*. at 500.15(a).

[23] *Id*. at 500.5(a-c).

[24] *Id*. at 500.13(a).

[25] *Id*. at 500.7(a).

[26] *Id*. at 500.1(n).

[27] *Id*. at 500.7(b).

[28] *Id*. at 500.20(b).

[29] Id. at 500.20(c).

Categories

Cybersecurity, Privacy & Data Protection | State Privacy Policy | Consumer Data Protection

LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.