PAUL HASTINGS

Stay Current

November 2023

Follow @Paul_Hastings

NYDFS Releases Major Update to Part 500 Cybersecurity Requirements for Financial Services Companies

By Aaron Charfoos, Jeremy Berkowitz & John J. Michels

The New York Department of Financial Services (NYDFS) adopted a long-expected amendment to its Part 500 Cybersecurity Regulations (Part 500) this week. These are the first significant changes to Part 500 since its inception in March 2017.

The draft amendment was first published for public comment on July 29, 2022, and was followed by two additional drafts (published on November 9, 2022 and June 28, 2023) reflecting responses to public comment and other changes. The finalized amendment, adopted on November 1, 2023, will go into effect immediately upon publication in the New York State Register; however, there are some transitional periods for when covered entities will need to demonstrate compliance with these provisions.

One of the major changes entails creating a new class of entities known as "Class A Companies" that will be subject to heightened requirements. Class A Companies are NYDFS-regulated businesses that either (a) have over 2,000 employees, or (b) have over $1 billion in gross annual revenue, in each case including the company's affiliates. The heightened requirements for Class A Companies include:

- Conducting an annual independent audit of their cybersecurity programs. These can be done by external or internal auditors.
- Implementing a privileged access management solution as well as methods for automatically blocking passwords that are commonly used.
- Implementing endpoint detection tools and other solutions to monitor and log potentially unauthorized activity.

There are also some significant updates in the area of governance and Chief Information Security Officer ("CISO") responsibilities that are applicable to all covered entities. In addition to an annual report, CISOs are now required to report to their senior governing body (e.g., board) or other senior executive on material cybersecurity issues including "significant cybersecurity events and significant changes to the covered entity's cybersecurity program."

The Part 500 update also includes requirements and guidance for how a senior governing body should "exercise oversight" of a covered entity's cybersecurity program. In particular, it requires the senior

governing body to have a "sufficient understanding of cybersecurity-related matters," receive regulatory updates on the cybersecurity program, and also provide sufficient resources for managing the program.

An overview of some other significant changes are listed in the table below:

Key Area	**Impact**
New Policy Requirements	Covered entities will need to develop new policies around end-of-life management, remote access, and vulnerability and patch management. These (and the remaining policies mandated by the Cybersecurity Regulation) must be approved annually by a senior governing body.
Asset Inventory	Covered entities will need to draft new procedures around maintaining a complete asset inventory including tracking information around: ▪ Asset owners; ▪ Asset locations; ▪ Asset classification or sensitivity; ▪ Asset support expiration data; and ▪ Asset recovery time objectives.
Extortion Payments	Covered entities are required to notify NYDFS within 24 hours of any "extortion payment," and, 30 days thereafter, provide a written description of the reasons that the payment was necessary, the alternatives that were considered, and the diligence that was performed with respect to the incident to ensure compliance with applicable law.
Multi-factor Authentication	Covered entities who fall under a certain employee and/or revenue threshold as noted in Section 500.19 must implement multi-factor authentication for remote access to both their information systems and third party applications, as well as all "privileged accounts other than service accounts that prohibit interactive login."
Limitations and Oversight of Privileged Accounts	The Part 500 update introduces a number of new technical safeguards that covered entities

Key Area	Impact
	will be required to implement, including limitations on the number and use of privileged accounts, a "password vaulting solution" for privileged accounts, and the use of multi-factor authentication for privileged accounts.
Risk Assessment Cadence	The Part 500 update requires covered entities to perform a risk assessment annually, instead of "periodically."
Business Continuity and Disaster Recovery	Covered entities must abide by a number of new requirements related to business continuity and disaster recovery plans, including the identification of essential data, facilities, infrastructure, and personnel; a communications plan; and procedures for maintenance of back-up facilities. The amendments also require that covered entities maintain backups that are isolated from network connections.

Effective Dates

Covered entities will need to demonstrate compliance within 180 days of the Part 500 update being published in the State Register, with the exception of the requirements listed in the table below:

Timeline	Requirements
November 1, 2023 (Immediately)	500.19(e-h): Various exemptions; 500.20: Enforcement requirements; 500.21: Effective date; 500.22: Compliance timeline; and, 500.24: Filing requirements.
30 Days from Publication in State Register	500.17: Notification of cybersecurity incidents to NYDFS.
One Year from Publication in State Register	500.4: CISO and senior governing body requirements; 500.15: Encryption requirements; 500.16: Incident response plan requirements; and,

Timeline	Requirements
	500.19(a): Exemptions based on employees and revenue.
18 Months from Publication in State Register	500.5(a)(2): Automated information systems scan requirements; 500.7: Privileged accounts requirements; 500.14(a)(2): Malicious code requirements; and, 500.15: Endpoint detection solution requirements.
Two Years from Publication in State Register	500.12: Multi-factor authentication requirements; and, 500.13(a): Asset inventory requirements.

Next Steps

Covered entities should begin to determine how the Part 500 updates may affect existing licenses or applications currently under review. In particular, covered entities should:

- Determine whether they fall under the definition of a "Class A Company."
- Update documentation to account for new policy and procedure requirements.
- Examine their cybersecurity governance structure to ensure that their CISOs and senior governing bodies have the capabilities and resources to manage the cybersecurity program and report on material issues as needed.

Paul Hastings' Data Privacy and Cybersecurity practice regularly advises on compliance with Part 500 and other cybersecurity regulations. If you have any questions concerning how the changes to Part 500 may affect your organization, please do not hesitate to contact the members of our team listed below.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings professionals:

Chicago

Aaron Charfoos
1.312.499.6016
aaroncharfoos@paulhastings.com

John J. Michels
1.312.499.6017
johnmichels@paulhastings.com

Washington, D.C.

Jeremy Berkowitz
1.202.551.1230
jeremyberkowitz@paulhastings.com