November 1, 2023
Vol. XLV
Issue 44

DEPARTMENT OF STATE
Division of Administrative Rules

NEW YORK STATE REGISTER

INSIDE THIS ISSUE:

- Academic Intervention Services
- Occupational Therapists' Authority to Provide Treatment for a Limited Time Without a Referral
- Requirements for Clinical Education and Simulation Experience in Nursing Education Program

Notice of Availability of State and Federal Funds

State agencies must specify in each notice which proposes a rule the last date on which they will accept public comment. Agencies must always accept public comment: for a minimum of 60 days following publication in the *Register* of a Notice of Proposed Rule Making, or a Notice of Emergency Adoption and Proposed Rule Making; and for 45 days after publication of a Notice of Revised Rule Making, or a Notice of Emergency Adoption and Revised Rule Making in the *Register*. When a public hearing is required by statute, the hearing cannot be held until 60 days after publication of the notice, and comments must be accepted for at least 5 days after the last required hearing. When the public comment period ends on a Saturday, Sunday or legal holiday, agencies must accept comment through the close of business on the next succeeding workday.

For notices published in this issue:

– the 60-day period expires on December 31, 2023
– the 45-day period expires on December 16, 2023
– the 30-day period expires on December 1, 2023

16. 'Lot of shellstock' or 'lot of shellfish' means a single type of bulk shellstock or containers of shellstock of not more than one day's harvest from a single defined harvest area gathered by one or more harvesters. A lot may also be used to segregate the harvest times and intended use for the purposes of complying with the time to temperature requirements.

17. 'Other deficiency' means a condition or practice that is not defined as critical or key but is not in accordance with the requirements of this Part.

18. 'Reshipper' means a shellfish dealer who receives and redistributes, in wholesale commerce, previously packed shellfish from a shipper, another reshipper or a processor. A reshipper is not authorized to pack, repack, tag or label, retag or re-label containers of shellfish. A reshipper is authorized to remove dead or broken shellfish from containers.

19. 'Shaded' means protected from exposure to sunlight that may cause a significant increase in post-harvest growth of 'Vibrio' bacteria due to an increase in temperature.

20. 'Shellfish' means, for the purpose of this Part, fresh or frozen oysters, clams, mussels or scallops or any edible portion thereof except for scallops when the final product is only the adductor muscle.

21. 'Shellfish sanitary inspection' means an unannounced/announced inspection of facilities, buildings, structures, records, invoices, shellfish tags and labels, hazard analysis, HACCP Plans and any other records required to be kept pursuant to this Part.

22. 'Shuck' means to release shellfish from one or both shells. 'Shucker' means a person who performs such activities.

23. 'Start of harvest' or 'time of harvest' means the time when the first shellstock is taken from the water, or in the case of intertidal harvest, the time of first exposure.

24. 'Transaction record' means a written or computer generated record of all shellfish received or shipped in wholesale or retail commerce.

25. 'Tributary' means a harbor, river, creek, pond, stream, etc. that is fed from a larger body of water such as a sound, ocean or bay.

26. 'Trip record' means a written document that includes the harvester name, harvester permit number, harvest area, the harvest date and time and, if applicable, the temperature of each lot of shellfish harvested.

27. 'Unwholesome' means the reverse of wholesome.

28. 'Vibrio parahaemolyticus Control Plan' ('Vp'CP) means a written plan developed by the department in response to a shellfish related 'Vp' illness outbreak or unacceptable risk of illness. Such plan outlines control measures that must be taken by shellfish harvesters and shellfish dealers to prevent or decrease the likelihood of 'Vp' related illnesses occurring due to the consumption of raw or undercooked shellfish.

29. 'Water storage' or 'wet storage' means the holding of shellstock harvested from certified shellfish lands in tanks of water or containers of shellstock harvested from certified shellfish lands held in certified bodies of water for purposes of storage /or de-sanding.

30. 'Wholesome' means shellfish that is fresh, unspoiled, clean and free from adulteration, contamination, evidence of previous temperature abuse and suitable for human consumption without altering its physical or organoleptic characteristics.

The following provisions have been added to 6 NYCRR sections 42.3 – 42.19:

1. More stringent shellfish identification requirements are described for shellfish harvesting, receiving, packing, and repacking operations, storage, and handling operations.

2. More stringent tagging requirements are added for shellfish harvesting, receiving, packing and repacking operations, shellfish storage, and shellfish handling operations.

3. Procedures that must be followed when the department has determined that shellfish might be hazardous for use as food for human consumption are detailed.

4. Shellfish harvesters and dealers will be required to apply time-temperature controls to keep shellfish cool after harvest, and during transportation and processing.

5. More detailed recordkeeping will be required for shellfish harvesters and dealers.

6. Certain designated shellfish harvest areas will be reduced in size and harvest area descriptions will be more clearly defined. This amendment will not result in any net change in the area available for shellfish harvest.

7. Provisions for protection of confidential shellfish landings data, statistics and other information provided by shellfish dealer permit holders to the department.

Final rule as compared with last published rule: Nonsubstantial changes were made in section 42.14(c)(3), (6), (9), (11), (13)(vi), (vii) and (ix).

Text of rule and any required statements and analyses may be obtained from: William M. Athawes, New York State Department of Environmental Conservation, 123 Kings Park Blvd. (Nissequogue River State Park), Kings Park, NY 11754, (631) 444-0494, email: william.athawes@dec.ny.gov

Additional matter required by statute: Pursuant to Article 8 of the ECL, the State Environmental Quality Review Act, a Coastal Assessment Form and a Short Environmental Assessment Form with a negative declaration have been prepared, and are on file with the Department.

Revised Regulatory Impact Statement, Regulatory Flexibility Analysis, Rural Area Flexibility Analysis and Job Impact Statement

Only non-substantive changes were made to the previously published proposed rule and no comments were received during the 60-day public comment period.

Non-substantive corrections were made to the description of harvest areas in 42.14(c)(3), (6), (9), (11), (13)(vi), (13)(vii), and (13)(ix). These non-substantive changes did not require any revisions to the previously published Regulatory Impact Statement, Regulatory Flexibility Analysis, Rural Area Flexibility Analysis and Job Impact Statement.

Initial Review of Rule

As a rule that requires a RFA, RAFA or JIS, this rule will be initially reviewed in the calendar year 2026, which is no later than the 3rd year after the year in which this rule is being adopted.

Assessment of Public Comment

The agency received no public comment.

Department of Financial Services

NOTICE OF ADOPTION

Cybersecurity Requirements for Financial Services Companies

I.D. No. DFS-45-22-00025-A
Filing No. 901
Filing Date: 2023-10-16
Effective Date: 2023-11-01

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following action:

Action taken: Amendment of Part 500 of Title 23 NYCRR.

Statutory authority: Financial Services Law, sections 102, 201, 202, 301, 302, 408; Banking Law, sections 10, 14, 37(3), (4), 44; Insurance Law, sections 109, 301, 308, 309, 316, 1109, 1119, 1503(b), 1717(b), 2110, 2127; arts. 21, 47 and 79

Subject: Cybersecurity Requirements for Financial Services Companies.

Purpose: To ensure that DFS-regulated entities most effectively address new and evolving cybersecurity threats.

Substance of final rule: Section 500.1 subdivisions (c-n) have been relettered, subdivision (l) has been removed, and new subdivisions (c), (d), (g), (h), (n) and (q) are added. Subdivision (l) is removed because "risk-based authentication" is a term no longer used in Part 500. Subdivision (c) is added to define "Chief Information Security Officer or CISO," which was previously defined in subdivision 500.4(a). Subdivision (d) is added to define a new category of covered entities, "class A companies," that are larger, more complex, and better-resourced entities that will be required to implement additional cybersecurity controls. Subdivision (g) is added to define "cybersecurity incident," derived from subdivision 500.17(a) with the addition of cybersecurity events that resulted in the deployment of ransomware within a material part of a covered entity's information systems. Subdivision (h) is added to define "independent audit." Subdivision (n) is added to define "privileged account." Subdivision (q) is added to define "senior governing body."

Subdivision 500.1(c), relettered as (e), is amended to clarify that the definition of covered entity applies to entities that are also regulated by other government agencies and is a non-substantive change.

Subdivision 500.1(f), relettered as (j), is amended to eliminate the reference to "text message on a mobile phone" and is a non-substantive change.

Subdivision 500.1(g), relettered as (k), is amended for a technical edit.

Subdivision 500.1(h), relettered as (l), is amended to clarify the definition of "penetration testing" and is a non-substantive change.

Subdivision 500.1(i), relettered as (m), is amended to remove the reference to non-governmental entities.

Subdivision 500.1(j), relettered as (o), is amended for a technical edit.

Subdivision 500.1(k), relettered as (p), is amended to clarify the definition of "risk assessment" and is a non-substantive change.

Subdivision 500.1(n), relettered as (s), is amended to exclude governmental entities from being third-party service providers and is a non-substantive change.

Subdivision 500.2(a) is amended to make a technical edit and clarify that covered entities shall maintain cybersecurity programs designed to protect their information systems and the nonpublic information ("NPI") stored on those systems and is a non-substantive change.

A new subdivision 500.2(c) is added to require that class A companies design and conduct independent audits of their cybersecurity programs.

Subdivision 500.2(c) is relettered as (d).

Subdivision 500.2(d), relettered as (e), is amended to clarify that covered entities adopting cybersecurity programs of their affiliates must provide the Superintendent, upon request, all documentation related to those programs and is a non-substantive change.

The section 500.3 introduction is amended to make technical edits and require a senior officer or the senior governing body to approve the written cybersecurity policies at least annually and require procedures to be developed and implemented pursuant to such policies. Section 500.3 subdivisions (b), (c), (d), (g), (h), (i), (l), (m) and (n) are amended, and a new subdivision (o) is added, to make technical edits and require cybersecurity policies and procedures address data retention, end of life management, remote access controls, systems monitoring, security awareness and training, application security, incident notification, and vulnerability management.

The title of section 500.4 is amended to read "Cybersecurity governance."

Subdivision 500.4(a) is amended for a technical edit because a new defined term "chief information security officer or CISO" was added as subdivision 500.1(c). Subdivision 500.4(b) is amended to require that the CISO's written report include plans for remediating material inadequacies and to clarify what the written report shall address.

New subdivisions 500.4(c) and (d) are added to require the CISO to timely report to the senior governing body on material cybersecurity issues and for the senior governing body to exercise oversight of cybersecurity risk management, including by having sufficient understanding of cybersecurity-related matters.

The title of section 500.5 is amended to read "Vulnerability management."

The section 500.5 introduction is amended to require written policies and procedures for vulnerability management and eliminate the exception to the requirements for penetration testing and vulnerability assessments if an entity employs effective continuous monitoring.

Subdivision 500.5(a) is amended for clarifying edits regarding penetration testing and to require such tests to be performed at least annually.

Subdivision 500.5(b), renumbered as 500.5(a)(2), is amended to make clarifying edits and require automated scans or manual reviews periodically and promptly after material system changes.

New subdivisions 500.5(b) and (c) are added to require that covered entities be promptly informed of new security vulnerabilities by having a monitoring process in place, and timely remediate vulnerabilities and give priority to remediation based on risk.

The title of section 500.7 is amended to read "Access privileges and management."

Section 500.7 is amended to add required controls regarding user and privileged accounts, protocols that permit remote control of devices, and passwords. Class A companies are also required to monitor privileged access activity and implement a privileged access management solution and an automated method of blocking commonly used passwords.

Subdivision 500.8(b) is amended to change the requisite timing from periodically to at least annually for reviewing, assessing, and updating written procedures, guidelines, and standards regarding development practices for in-house developed applications, and the security of externally developed applications utilized by the covered entity.

Subdivision 500.9(a) is amended for a technical edit and to require covered entities' risk assessments to be reviewed and updated at least annually and whenever a change in the business or technology causes a material change to their cyber risk.

Subdivision 500.10(a) is amended for a technical edit.

Subdivision 500.10(b) is amended for a technical edit and to require covered entities to incorporate the requirements of section 500.4 when relying on an affiliate or third party to assist in complying with Part 500.

Subdivisions 500.11(a) and (b) are amended for technical edits.

Subdivision 500.11(c) is removed because it was duplicative of subdivision 500.19(b) and is a non-substantive change.

Subdivision 500.12(a) is removed.

Subdivision 500.12(b), relettered as (a), is amended to require multi-factor authentication for any individual accessing any information systems of a covered entity, unless the covered entity qualifies for a limited exemption pursuant to subdivision 500.19(a), in which case multi-factor authentication shall be utilized for remote access to the covered entity's information systems, third-party applications from which NPI is accessible, and all privileged accounts other than service accounts that prohibit interactive login.

A new subdivision 500.12(b) is added to allow the CISO to approve reasonably equivalent or more secure compensating controls, which must be reviewed at least annually.

The title of section 500.13 is amended to read "Asset management and data retention requirements."

A new subdivision 500.13(a) is added to require covered entities to maintain an asset inventory.

Subdivision 500.13(a), relettered as (b), is amended for a technical edit.

The title of section 500.14 is amended to read "Monitoring and training."

Subdivision 500.14(a) is amended to make technical edits, incorporate subdivision (b), and require covered entities to implement controls designed to protect against malicious code and provide cybersecurity awareness training that includes social engineering at least annually.

A new subdivision 500.14(b) is added to require class A companies to implement, unless the CISO has approved in writing the use of reasonably equivalent or more secure compensating controls, an endpoint detection and response solution to monitor anomalous activity, and a centralized logging and security event alerting solution.

Subdivision 500.15(a) is amended to require covered entities to implement written policies requiring encryption that meets industry standards.

Paragraph 500.15(a)(1) is removed to eliminate the ability to use compensating controls for encryption of NPI in transit.

Paragraph 500.15(a)(2), relettered as (b), is amended to require the CISO's written approval of the effectiveness of compensating controls.

Subdivision 500.15(b) is removed.

The title of section 500.16 is amended to read "Incident response and business continuity management."

Subdivision 500.16(a) is amended to require written plans that contain proactive measures to investigate and mitigate cybersecurity events and to ensure operational resilience, including incident response, business continuity and disaster recovery ("BCDR") plans.

A new paragraph 500.16(a)(1) is added that incorporates subdivision 500.16(b) and requires incident response plans to also address recovery from backups, preparing root cause analysis, and updating the plan as necessary.

A new paragraph 500.16(a)(2) is added to require covered entities to establish BCDR plans.

New subdivisions 500.16(b), (c), (d), and (e) are added to require: copies of the plans to be made accessible to relevant employees, employee training for implementing the plans, testing of incident response and BCDR plans and ability to restore from backups at least annually with staff and management critical to the response and revising those plans as necessary, and maintaining backups necessary to restore material operations that are adequately protected from unauthorized alterations or destruction.

Subdivision 500.17(a) is amended to make technical edits because a new defined term "cybersecurity incident" was added as subdivision 500.1(g) and to require notice of a cybersecurity incident that occurred at the covered entity, its affiliates, or a third-party service provider to be submitted to DFS electronically in the form set forth on the Department's website ("electronic submission").

A new paragraph 500.17(a)(2) is added to require covered entities to promptly provide information regarding the cybersecurity event when requested.

Subdivision 500.17(b) is amended to require electronic submission of either a certification of compliance or an acknowledgment of noncompliance that is signed by the covered entity's highest-ranking executive and CISO or the senior officer responsible for its cybersecurity program. Covered entities must maintain information supporting their submissions including all remedial efforts undertaken to address any areas, systems and processes that required material improvement, updating or redesign.

A new subdivision 500.17(c) is added to require covered entities to provide electronic notice to the Superintendent of an extortion payment within 24 hours of such payment, and additional information within 30 days of such payment including a written description of the reasons payment was necessary, a description of alternatives to payment considered, all diligence performed to find alternatives to payment, and all diligence performed to ensure compliance with applicable rules and regulations including those of the Office of Foreign Assets Control.

Subdivision 500.19(a) is amended to expand the limited exemption to include entities with fewer than 20 employees and independent contractors, businesses with less than $7,500,000 in gross annual revenue, and businesses with less than $15,000,000 in year-end total assets, and to provide that the requirements contained in section 500.12 and paragraph 500.14(a)(3) are not exempted.

Subdivision 500.19(b) is amended to exempt wholly owned subsidiaries, to the extent they are covered by their parent's cybersecurity program and their parent is a covered entity.

A new subdivision 500.19(e) is added to exempt inactive insurance brokers from the requirements of Part 500.

Subdivision 500.19(e), relettered as (f), is amended to require Notices of Exemptions to be filed electronically in the form set forth on the Department's website.

Subdivision 500.19(f), relettered as (g), is amended to add reciprocal jurisdiction reinsurers recognized pursuant to 11 NYCRR Part 125, individual insurance agents placed in inactive status under Insurance Law section 2103, and individual licensees placed in inactive status under Banking Law section 599-i to the persons exempt from the requirements of Part 500.

Subdivision 500.19(g) is relettered as (h) and amended to require covered entities to comply with the requirements of Part 500 within 180 days of ceasing to qualify for an exemption.

Subdivision 500.20 is amended to define what constitutes a violation of Part 500 and to list the factors the Superintendent shall take into account when assessing penalties.

Subdivision 500.21(a) is amended for a technical edit.

A new subdivision 500.21(b) is added to establish the effective date of the second amendment to Part 500.

New subdivisions 500.22(c), (d) and (e) are added to establish the timeframe covered entities will have from the effective date of the second amendment to Part 500 to comply with its new requirements.

A new section 500.24 entitled "Exemptions from electronic filing and submission requirements" is added to permit covered entities to request an exemption to electronic filing.

Appendices A and B, which are forms for certifications of compliance and notices of exemption, are repealed. Such forms will be set forth on the Department's website, as is current practice.

Final rule as compared with last published rule: Nonsubstantial changes were made in sections 500.1-500.5, 500.7, 500.8(b), 500.9(a), 500.10-500.17, 500.19-500.22, 500.24 and Appendices A and B.

Revised rule making(s) were previously published in the State Register on June 28, 2023.

Text of rule and any required statements and analyses may be obtained from: Joanne Berman, New York State Department of Financial Services, One State Street, New York, NY 10004, (917) 991-6965, email: Joanne.Berman@dfs.ny.gov

Revised Regulatory Impact Statement, Regulatory Flexibility Analysis, Rural Area Flexibility Analysis and Job Impact Statement

A revised Regulatory Impact Statement, Regulatory Flexibility Analysis, Rural Area Flexibility Analysis and Job Impact Statement is not required for the adoption of the second amendment to 23 NYCRR 500 because the non-substantive revisions to the regulation do not require a change to the previously published Regulatory Impact Statement, Regulatory Flexibility Analysis, Rural Area Flexibility Analysis and Job Impact Statement.

Initial Review of Rule

As a rule that requires a RFA, RAFA or JIS, this rule will be initially reviewed in the calendar year 2026, which is no later than the 3rd year after the year in which this rule is being adopted.

Assessment of Public Comment

The New York State Department of Financial Services ("DFS") received comments from banking, insurance, and other industry groups, regulated organizations, unregulated businesses, and members of a law school law society.

Commenters stated their support for the following changes in the Cybersecurity Regulation: (1) providing clarification that only those affiliates sharing information systems, cybersecurity resources, or all or any part of a cybersecurity program with a covered entity should be included when calculating the number of employees and gross annual revenue in the definition of "class A companies"; (2) including audits conducted by internal auditors in the definition of "independent audit"; (3) removing accounts that can affect a material change to the technical or business operations of the covered entity from the definition of "privileged account"; (4) removing the requirement that the senior governing body "provide direction to management" on a covered entity's cybersecurity risk management in § 500.4(d); (5) replacing the senior governing body's obligation to have "sufficient expertise and knowledge" with the obligation instead to have "sufficient understanding" of cybersecurity-related matters in § 500.4(d); (6) removing the requirement for class A companies to use external experts to conduct a risk assessment at least once every three years in § 500.9; (7) clarifying that the privileged accounts for which limited exempt entities must use multi-factor authentication in § 500.12(a)(3) do not include "service accounts that prohibit interactive login"; (8) adding requirements for class A companies to implement endpoint detection and response solutions and solutions that centralize logging in § 500.14; (9) clarifying that covered entities only need to establish the requisite incident response and business continuity and disaster recovery plans in § 500.16(a) for "cybersecurity events" and not all "disruptive events;" (10) clarifying that covered entities can submit their certification of compliance required by § 500.17(b) as long as they "materially complied with" the requirements of Part 500 "during the prior calendar year;" and (11) adding the requirement that a failure to comply for any 24-hour period with any section of Part 500 must be material to constitute a violation in § 500.20(b)(2).

Commenters generally requested that DFS continue to take a risk-based approach to cybersecurity; align Part 500 with other cybersecurity rules and frameworks, such as the cybersecurity rules promulgated by the U.S. Securities and Exchange Commission and the frameworks published by the National Institute of Standards and Technology ("NIST"), including the draft NIST Cybersecurity Framework 2.0; increase collaboration between DFS and its regulated entities; and describe how covered entities can meet their responsibilities under Part 500, recommend additional cybersecurity steps they can take, and include reference points of a "mature" program.

DFS received additional comments that it addresses in the complete version of the APC that DFS posted on its website at: https://www.dfs.ny.gov/industry_guidance/regulatory_activity/financial_services

NOTICE OF ADOPTION

Financial Statement Filings and Accounting Practices and Procedures

I.D. No. DFS-31-23-00004-A

Filing No. 900

Filing Date: 2023-10-16

Effective Date: 2023-11-01

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following action:

Action taken: Amendment of Part 83 (Regulation 172) of Title 11 NYCRR.

Statutory authority: Financial Services Law, sections 202, 302; Insurance Law, sections 107(a)(2), 301, 307, 308, 1109, 1301, 1302, 1308, 1404, 1405, 1407, 1411, 1414, 1501, 1505, 3233, 4117, 4233, 4239, 4301, 4310, 4321-a, 4322-a, 4327, 6404; Public Health Law, art. 44

Subject: Financial Statement Filings and Accounting Practices and Procedures.

Purpose: To update reference to NAIC AP&P Manual as of date from March 2021 to March 2023, and other non-substantive changes.

Text or summary was published in the August 2, 2023 issue of the Register, I.D. No. DFS-31-23-00004-P.

Final rule as compared with last published rule: No changes.

Text of rule and any required statements and analyses may be obtained from: Michael Campanelli, Department of Financial Services, One State Street, New York, NY 10004, (212) 480-5290, email: Michael.Campanelli@dfs.ny.gov

Assessment of Public Comment

The agency received no public comment.

Office for People with Developmental Disabilities

NOTICE OF ADOPTION

Waiver Eligibility

I.D. No. PDD-21-23-00004-A

Filing No. 896

Filing Date: 2023-10-11

Effective Date: 2023-11-01

PURSUANT TO THE PROVISIONS OF THE State Administrative Procedure Act, NOTICE is hereby given of the following action:

Action taken: Amendment of section 635-10.3 of Title 14 NYCRR.

Statutory authority: Mental Hygiene Law, sections 13.07, 13.09(b) and 16.00

Subject: Waiver eligibility.

Purpose: To use gender neutral language and coincide with SSL 366(7-a)(b).