Summary of Proposed New 23 NYCRR 500.

The following is a summary of the proposed rule:

Section 500.00, “Introduction,” introduces the proposed rule.

Section 500.01, “Definitions,” defines terms used throughout the proposed rule.

Section 500.02, “Cybersecurity Program,” requires that each Covered Entity maintain a cybersecurity program reasonably designed to protect the confidentiality, integrity and availability of its Information Systems.

Section 500.03, “Cybersecurity Policy,” requires each Covered Entity to implement and maintain a written cybersecurity policy addressing specified areas and also sets forth the requirements for approval of that policy.

Section 500.04, “Chief Information Security Officer,” requires that each Covered Entity designate a qualified individual responsible for overseeing and implementing the Covered Entity’s cybersecurity program (the “CISO”), and that the CISO shall develop a written report, at least annually, which shall be reviewed internally and which shall address specified cybersecurity issues.

Section 500.05, “Penetration Testing and Vulnerability Assessments,” requires each Covered Entity’s cybersecurity program to include monitoring and testing, developed in accordance with the Covered Entity’s Risk Assessment, designed to assess the effectiveness of the Covered Entity’s cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments, and shall be done periodically. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct annual penetration testing and a bi-annual vulnerability assessments of the Covered Entity’s Information Systems, based on the Covered Entity’s Risk Assessment.

Section 500.06, “Audit Trail,” requires each Covered Entity to securely maintain systems that, based on its Risk Assessment, reconstruct material financial transactions and include audit trails designed to detect and respond to Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operations of the Covered Entity.

Section 500.07, “Access Privileges,” requires that each Covered Entity shall, based on the Covered Entity’s Risk Assessment, limit user access privileges to Information Systems that provide access to Nonpublic Information and that the Covered Entity shall periodically review such privileges.

Section 500.08, “Application Security,” requires that each Covered Entity’s cybersecurity program include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity’s technology environment, and also requires that such procedures and standards be periodically reviewed, assessed and updated.

Section 500.09, “Risk Assessment,” requires each Covered Entity to conduct a periodic Risk Assessment of the Covered Entity’s Information Systems, updated as reasonably necessary to address changes to the Covered Entity’s Information Systems, Nonpublic Information or business operations. The Risk Assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the Covered Entity’s business operations related to cybersecurity, Nonpublic Information collected or stored, Information Systems utilized and the availability and effectiveness of controls to protect Nonpublic Information and Information Systems. The Risk Assessment shall be documented and shall be carried out in accordance with written policies and procedures which shall include criteria for the evaluation and categorization of identified cybersecurity risks or threats facing the Covered Entity, criteria for assessing the confidentiality, integrity, security and availability of the Covered Entity’s Information Systems and Nonpublic Information, and requirements describing how identified risks will be mitigated or accepted, and how the cybersecurity program will address the risks.

Section 500.10, “Cybersecurity Personnel and Intelligence,” requires each Covered Entity to utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate, or a Third Party Service Provider; provide such personnel with cybersecurity updates and training; and verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

Section 500.11, “Third Party Service Provider Security Policy,” requires each Covered Entity to develop policies and procedures designed to ensure the security of Information Systems and Nonpublic Information accessible to, or held by, Third Party Service Providers. Such policies shall be based on the Covered Entity’s Risk Assessment and shall include relevant guidelines for due diligence and/or contractual protections relating to Third Party Service Providers.

Section 500.12, “Multi-Factor Authentication,” requires each Covered Entity to use effective controls to protect against unauthorized access to Nonpublic Information or Information Systems. Covered Entities are required to utilize Multi-Factor Authentication for any individual accessing the Covered Entity’s internal networks from an external network, unless the Covered Entity’s CISO has approved in writing the use of reasonably equivalent or more secure access controls.

Section 500.13, “Limitations on Data Retention,” requires each Covered Entity to have policies and procedures for the secure periodic disposal of specified categories of Nonpublic Information.

Section 500.14, “Training and Monitoring,” requires each Covered Entity to implement risk-based policies to monitor the activity of Authorized Users and detect unauthorized access or use of Nonpublic Information, and to provide for regular cybersecurity awareness training for all personnel.

Section 500.15, “Encryption of Nonpublic Information,” requires each Covered Entity to implement controls, including encryption, based on the Covered Entity’s Risk Assessment, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest. This section allows for the use of effective compensating controls to secure Nonpublic Information in transit over external networks and at rest if encryption of such is infeasible. Such compensating controls must be reviewed and approved by the Covered Entity's CISO. To the extent that a Covered Entity is utilizing compensating controls, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

Section 500.16, "Incident Response Plan," requires each Covered Entity to establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event materially affecting the confidentiality, integrity or availability of the Covered Entity's Information Systems or the continuing functionality of any aspect of the Covered Entity's business or operations.

Section 500.17, "Notices to Superintendent," requires each Covered Entity to annually submit to the Superintendent a written statement by February 15, certifying that the Covered Entity is in compliance with the requirements set forth in the proposed rule; to maintain for examination by the Department all records, schedules and data supporting the certificate for a period of five years; to notify the superintendent within 72 hours from the determination of the occurrence of a Cybersecurity Event of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body, or that has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity; and to document the identification of areas that require material improvement, updating or redesign, as well as planned remedial efforts.

Section 500.18, "Confidentiality," states that information provided by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under the Banking Law, Insurance Law, Financial Services Law, Public Officers Law, or any other applicable state or federal law.

Section 500.19, "Exemptions," provides that Covered Entities that have less than the specified number of employees, gross annual revenue, or year-end total assets shall be exempt from the requirements of the enumerated sections; an exemption for an employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity; an exemption from enumerated sections for a Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess Nonpublic Information; a requirement that Covered Entities that qualify for an exemption file a Notice of Exemption; and that a Covered Entity that ceases to qualify for an exemption must comply with all applicable requirements of the proposed rule.

Section 500.20, “Enforcement,” provides that the proposed rule will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent’s authority under any applicable laws.

Section 500.21, “Effective Date,” provides that the proposed rule will be effective March 1, 2017, and that Covered Entities will be required to annually prepare and submit a certification of compliance pursuant to Section 500.17 commencing February 15, 2018.

Section 500.22, “Transitional Periods,” provides that Covered Entities shall have 180 days from the effective date of the proposed rule to comply with its requirements, except as otherwise specified, and also includes additional transitional periods.

Section 500.23, “Severability,” states that in the event a specific provision of the proposed rule is adjudged invalid, such judgment shall not impair the validity of the remainder of the proposed rule.