Summary of New 23 NYCRR 500.

The following is a summary of the final rule:

Section 500.00, “Introduction,” introduces the rule.

Section 500.01, “Definitions,” defines terms used throughout the 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. 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 assessment 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 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 covering the prior calendar year by February 15, certifying that the Covered Entity is in compliance with the requirements set forth in the 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 impacting the Covered Entity 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; an exemption from enumerated sections for a Covered Entity under Article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates); a requirement that Covered Entities that qualify for an exemption file a Notice of Exemption; an exemption for Persons that do not otherwise qualify as Covered Entities and are subject to Insurance Law Section 1110, Insurance Law Section 5904, and any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125; and that a Covered Entity that ceases to qualify for an exemption must comply with all applicable requirements of the final rule.

Section 500.20, "Enforcement," provides that the 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 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 final 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 rule is adjudged invalid, such judgment shall not impair the validity of the remainder of the rule.

Assessment of Public Comments to the Revised Rule Making for New Part 500 to 23 NYCRR.

The New York State Department of Financial Services (the "Department" or "DFS") initially released proposed rule 23 NYCRR 500 in September 2016 and received over 150 comments to that proposed rulemaking from individuals and entities, including a variety of regulated entities and trade associations, as well as from third party service providers, including cybersecurity service providers, and others. Every comment was processed and considered by the Department and in December 2016 the Department issued a revised proposed rule 23 NYCRR 500, which incorporated a number of changes made in response to those comments. In response to that revised proposed rulemaking the Department received more than 60 comments from many of the same commenters. Many commenters addressed more than one provision of the proposed regulation, and many requested specific changes. The Department has processed and considered every comment and has made several clarifications to the regulation. This summary is intended to provide an overview of the categories of comments received by the Department, the clarifications the Department has added to the final rule in response to those comments, and, where applicable, the reasons for not making additional changes or clarifications.

Generally, comments received during the second comment period addressed issues regarding the scope, meaning and/or particular wording of nearly every section of the revised proposed rule. In many cases, the Department did not make suggested revisions because the Department determined, based on its experience and knowledge, that the suggestions were unnecessary within the context of the final rule or were inconsistent with the minimum cybersecurity standards the Department is setting.

Many commenters commended the Department for its efforts in addressing cybersecurity. Many commenters also expressed broad support for changes made, recognizing the Department's responsiveness to comments submitted and praising the Department's efforts and process.

Some commenters stated that the proposed regulation should harmonize more closely with other standards, including state, federal and international standards, both existing and proposed. Several commenters

also stated that the Department should wait for the federal government to promulgate regulations or should be allowed to comply with alternative standards currently used in industry in lieu of the standards contained in the revised proposed rule. The Department has not accepted any such suggestions, as the Department continues to believe that the regulation is consistent with other standards, and it is vitally important to establish regulatory minimum standards for cybersecurity practices to address challenges currently facing the New York financial services sector.

Commenters requested clarification, tailoring and/or narrowing of certain definitions, including the definitions of "Cybersecurity Event," "Information System," "Nonpublic Information" and "Publicly Available Information." DFS has not revised these definitions because the Department believes the breadth of these definitions are appropriate in the final rule and should not be narrowed or limited.

Some commenters also suggested that the definition of "Penetration Testing" was unclear or overly narrow with respect to testing methodologies. In response, the Department revised section 500.01(i) to delete the word "unauthorized" as unnecessarily limiting.

Several commenters requested clarification regarding the allocation of responsibilities for the provisions of the Cybersecurity Program section with respect to Affiliates. In response the Department revised section 500.02(c) to clarify that a Covered Entity may adopt the relevant and applicable provisions of the cybersecurity program of an Affiliate provided that such provisions meet the requirements of the final rule.

Commenters made suggestions in regard to the Cybersecurity Policy section (500.03), including suggested revisions to narrow its scope or incorporate other standards. The Department considered these comments and has decided not to narrow section 500.03, because the Department has determined that its provisions are appropriately consistent with the Department's goal of requiring entities to have a broad, risk based cybersecurity program.

Commenters made suggestions or sought clarification in regard to the Chief Information Security Officer section (500.04), particularly with respect to its scope. The Department did not make any changes in response, as the Department believes that this section's scope is appropriate and sufficiently clear.

Several commenters requested clarification regarding the requirements of the Penetration and Vulnerability Assessment section (500.05), including comments relating to timing requirements. In response, the Department revised section 500.05 to clarify that periodic penetration testing and vulnerability assessments are required in the absence of continuous monitoring capabilities.

Some commenters asserted that the requirements of the Audit Trail section (500.06) were overly broad, leading to the capture and retention of too much information. In addition, some commenters claimed that the five-year retention period was unnecessarily long. In response, the Department has made certain revisions to section 500.06, including decreasing the retention period applicable to paragraph 500.06(a)(2) to three years.

Commenters made suggestions in regard to the Application Security section (500.08), including suggested revisions to narrow its scope. The Department has not revised section 500.08 in response, because the Department has determined that its provisions are appropriately consistent with the Department's goal of setting effective minimum standards.

Commenters also made suggestions or sought clarification in regard to the Risk Assessment section (500.09), particularly with respect to its scope. The Department did not make any changes in response, as the Department believes that this section's scope is appropriate and sufficiently clear.

Commenters offered suggestions regarding the Cybersecurity Personnel and Intelligence section (500.10), including suggestions that it be narrowed or that more specific language be included. The Department did not make any changes in response, as the Department believes that the section is appropriate. However, the Department did make a clarifying revision.

Commenters also stated that the requirements in section 500.11 regarding third parties doing business with a Covered Entity were too prescriptive, requiring entities to apply certain controls to all Third Party Service Providers and subjecting such Third Party Service Providers to multiple conflicting requirements imposed by multiple Covered Entities. Commenters also requested clarification regarding several subsections, including the definitions of the terms "Multi-Factor Authentication" and "sensitive systems" as used in section 500.11. The Department has clarified section 500.11 by, among other things, making greater use of previously defined terms. The Department notes that, as revised, section 500.11 requires Covered Entities to develop and implement risk-based policies and procedures that include relevant guidelines concerning certain enumerated issues.

In addition, commenters suggested revisions to the Multi-Factor Authentication section (500.12), asserting both that its provisions should be less prescriptive and more prescriptive. The Department did not make any changes in response, as the Department believes that section 500.12 is appropriately tailored.

Commenters made suggestions or sought clarification in regard to the Limitations on Data Retention section (500.13), particularly with respect to its scope. The Department did not make any changes in response, as the Department believes that this section's scope is appropriate and sufficiently clear.

Commenters also made suggestions and sought clarification in regard to the Training and Monitoring section (500.14). In response, the Department made a clarifying revision.

Several commenters requested changes in scope or wording to the Encryption of Nonpublic Information section (500.15), suggesting, for example, that the encryption at rest language should be removed altogether or should be limited in application, or that the provisions regarding encryption of data in transit should be revised to exclude leased lines from the term "external networks." The Department has not revised section 500.15 in response to these comments because the Department has determined that section 500.15 as drafted appropriately highlights the importance of encryption as a key cybersecurity control while also providing flexibility for Covered Entities to evaluate, in light of their Risk Assessment, the scope and means of feasibly implementing encryption

controls. Further, the Department does not believe the term “external networks,” which includes both public networks and external leased lines, requires further clarification within the final rule.

Commenters made suggestions in regard to the Incident Response Plan section (500.16), including suggested revisions to narrow its scope. The Department has not revised section 500.16 in response, because the Department has determined that its provisions are appropriately consistent with the Department’s goal of setting effective minimum standards.

Commenters requested clarification with respect to provisions of the Notices to the Superintendent section (500.17) and also offered suggestions to narrow its scope and suggestions to increase the 72-hour reporting timeframe. Based on its experience and goals, the Department believes that the 72-hour reporting timeframe is appropriate and necessary to address fast-moving cybersecurity risks and thus has retained it. However, in response to comments, the Department has made revisions to section 500.17 to clarify the scope of reportable Cybersecurity Events.

Some commenters asserted that the annual certification requirement of subsection 500.17(b) should be eliminated. Other commenters sought revisions in the annual certification requirement and/or certification form. The Department has determined that the annual certification is an important requirement for effective regulatory oversight of cybersecurity within and the Department’s overall oversight of the financial markets and is essential to good corporate governance. Accordingly, the Department has retained this requirement, but has made revisions to this section to clarify the time period covered by the certification.

Commenters offered suggestions regarding the Confidentiality section (500.18), including suggestions that it be expanded or that more specific language be included. The Department did not make any changes in response, as the Department believes that the current Confidentiality section is sufficient.

The Department received a number of comments regarding coverage of the regulation and its limited exemptions. Certain types of entities asserted that they should not be considered, or were not, a "Covered Entity." Others sought clarification as to whether or not they were a "Covered Entity" Others requested clarification or offered suggestions regarding the calculation of eligibility for the limited exemptions set forth in subsection 500.19(a). Some commenters questioned whether the revised proposed regulation extended to entities or activities outside of the jurisdiction of the Department, or regarding which state regulation has been preempted by federal law. As with all regulations, the Department does not intend to extend the application of the final rule beyond the Department's legal boundaries and wants them to extend to entities that are appropriate.

The Department has revised section 500.19 to clarify the scope of the regulation. More specifically, the Department has revised section 500.19 to include appropriate exemptions for:

- Entities regulated under Article 70 of the New York Insurance Law (captive insurance companies);
- Entities regulated under section 1110 of the New York Insurance Law (charitable annuity societies);
- Entities regulated under section 5904 of the New York Insurance Law (non-domestic risk retention groups); and
- Any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125.

In addition, the Department has clarified the limited exemptions including by limiting exemptions to activities within New York, and clarifying whether affiliates should be included in those calculations. In response, the Department has made certain changes to subsection 500.19(a) to clarify its scope and application.

Commenters additionally requested clarification regarding the timing of filing the required notice of exemption under section 500.19(e). In response, the Department revised section 500.19(e) to clarify that the required filing must be made within 30 days of the determination that the Covered Entity is exempt.

Some commenters offered suggestions for more-specific enforcement-related provisions. The Department did not make any revisions in response to those suggestions because it believes that the current Enforcement section (500.20) is sufficient.

Several commenters expressed concern about the implementation timeframes contained in sections 500.21 and 500.22 and requested that various transitional periods be extended or otherwise adjusted. The Department has determined that the effective date of the final rule and the various transitional periods are appropriate.

..

Regulatory Impact Statement for New 23 NYCRR 500.

Statement as to why a Revised Regulatory Impact Statement (RIS) is not required:

A Revised RIS is not required because the revisions to the proposed regulation do not change the conclusions set forth in the previously published RIS.

Regulatory Flexibility Analysis for Small Businesses and Local Governments for New 23 NYCRR 500.

Statement as to why a Revised Regulatory Flexibility Analysis (RFA) is not required:

A Revised RFA is not required because the revisions to the proposed regulation do not change the conclusions set forth in the previously published RFA.

Job Impact Statement for New 23 NYCRR 500.

Statement as to why a Revised Job Impact Statement is not required:

A Revised Job Impact Statement is not required because the revisions to the proposed regulation do not change the statement regarding the need for a Job Impact Statement that was previously published.

Rural Area Flexibility Analysis for New 23 NYCRR 500.

Statement as to why a Revised Rural Area Flexibility Analysis (RAFA) is not required:

A Revised RAFA is not required because the revisions to the proposed regulation do not change the conclusions set forth in the previously published RAFA.