plan year. However, the Department is concerned about the disproportionate impact that federal risk adjustment may have on carriers in the New York market and possible unnecessary instability in the health insurance market that would adversely impact insureds. As a result, the Department determined that it is necessary to establish a market stabilization pool for the small group health insurance market.

The Department also considered a cap of other than 30% of the amount to be received from the federal risk program, with regard to the uniform percentage of the payment transfer for the market stabilization pool under this rule. However, Department actuaries considered the fact that (1) the federal risk adjustment program calculates risk scores and payments transfers based in part upon a medical loss ratio computation that includes administrative expenses, profits, and claims, and (2) it does not appear to fully address New York's rating tier structure. The actuaries determined that up to 30% of the amount to be received from the federal risk adjustment program is the maximum amount that would be necessary for a payment transfer under this rule.

9. Federal standards: The rule does not exceed any minimum standards of the federal government for the same or similar subject areas. Rather, the amendment to the rule complements the federal risk adjustment program.

10. Compliance schedule: The Department is promulgating this rule on an emergency basis so that the Superintendent may establish a New York risk adjustment pool for plan year 2017 if the Superintendent determines that it will be necessary following CMS's annual release of the federal risk adjustment results for the 2017 plan year. If the Superintendent does establish the pool, carriers will have to comply in 2018.

Regulatory Flexibility Analysis

Small businesses: The Department of Financial Services finds that this rule will not impose any adverse economic impact on small businesses and will not impose any reporting, recordkeeping, or other compliance requirements on small businesses. The basis for this finding is that this rule is directed at insurers and health maintenance organizations ("HMOs") that elect to issue policies or contracts subject to the rule. Such insurers and HMOs do not fall within the definition of "small business" as defined by State Administrative Procedure Act § 102(8), because in general they are not independently owned and do not have fewer than 100 employees.

Local governments: The rule does not impose any impact, including any adverse impact, or reporting, recordkeeping, or other compliance requirements on any local governments. The basis for this finding is that this rule is directed at insurers and HMOs that elect to issue policies or contracts subject to the rule.

Rural Area Flexibility Analysis

1. Types and estimated numbers of rural areas: Insurers and health maintenance organizations ("HMOs") (collectively, "carriers") affected by this rule operate in every county in this state, including rural areas as defined by State Administrative Procedure Act § 102(10).

2. Reporting, recordkeeping and other compliance requirements; and professional services: The rule imposes additional reporting, recordkeeping, and other compliance requirements by requiring carriers, including carriers located in rural areas, designated as receivers of a payment transfer from the federal risk adjustment program, to remit a uniform percentage of that payment transfer to the Superintendent of Financial Services ("Superintendent") as determined by the Superintendent. However, no carrier, including carriers in rural areas, should need to retain professional services to comply with this rule.

3. Costs: This rule imposes compliance costs on carriers that elect to issue policies or contracts subject to the rule, including carriers in rural areas. The costs are difficult to estimate and will vary from carrier to carrier depending on the impact of the federal risk adjustment program on the market, including federal payment transfers, statewide average premiums, and the ratio of claims to premiums. However, any additional costs to carriers in rural areas should be the same as for carriers in non-rural areas.

4. Minimizing adverse impact: This rule uniformly affects carriers that are located in both rural and non-rural areas of New York State. The rule should not have an adverse impact on rural areas.

5. Rural area participation: The Department of Financial Services ("Department") is promulgating this rule on an emergency basis because carriers soon will begin binding coverage for policies written outside of the health exchange. In addition, the New York State of Health, the official health insurance marketplace, has set September 9, 2016 as the date by which carriers must commit to selling certain policies or contracts on the health exchange. In order to implement the rule for the 2017 plan year and to minimize market issues, it is imperative that this rule be promulgated on an emergency basis. Carriers in rural areas will have an opportunity to participate in the rule making process when the proposed rule is published in the State Register and posted on the Department's website.

Job Impact Statement

This rule should not adversely impact jobs or employment opportunities in New York State. This rule authorizes the Superintendent of Financial Services ("Superintendent") to implement a market stabilization pool for the small group health insurance market if, after reviewing the impact of the federal risk adjustment program on this market, the Superintendent determines that a market stabilization mechanism is a necessary amelioration. This rule prudently ameliorates a possible disproportionate impact that federal risk adjustment may have on insurers and health maintenance organizations, addresses the needs of the small group health insurance market in New York, and prevents unnecessary instability in the health insurance market.

REVISED RULE MAKING
NO HEARING(S) SCHEDULED

Cybersecurity Requirements for Financial Services Companies

I.D. No. DFS-39-16-00008-RP

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

Proposed Action: Addition of Part 500 to Title 23 NYCRR.

Statutory authority: Financial Services Law, sections 102, 201, 202, 301, 302 and 408

Subject: Cybersecurity requirements for financial services companies.

Purpose: To require effective cybersecurity to protect consumers and ensure the safe and sound operation of Department-regulated entities.

Substance of revised rule: 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.

Revised rule compared with proposed rule: Substantial revisions were made in sections 500.11, 500.15, 500.21 and 500.22.

Text of revised proposed rule and any required statements and analyses may be obtained from Cassandra Lentchner, New York State Department of Financial Services, One State Street, New York, NY 10004, (212) 709-1675, email: CyberRegComments@dfs.ny.gov

Data, views or arguments may be submitted to: Same as above.

Public comment will be received until: 30 days after publication of this notice.

Revised Regulatory Impact Statement

1. Statutory Authority: In Section 102 of the New York Financial Services Law (the "Financial Services Law" or "FSL"), the legislature declares that the purpose of the FSL is "to ensure the continued safety and soundness of New York's banking, insurance and financial services industries, as well as the prudent conduct of the providers of financial products and services, through responsible regulation and supervision." Pursuant to FSL Section 201, the Department of Financial Services (the "Department") has broad authority to take such actions as are necessary to ensure the continued solvency, safety, soundness and prudent conduct of the providers of financial products and services; to protect users of financial products and services from financially impaired or insolvent providers of such services; and to eliminate financial fraud, other criminal abuse and unethical conduct in the industry. Further, FSL Section 301 gives the Department broad power "to protect users of financial products and services." In addition, FSL Section 302 provides the Department with equally broad authority to adopt regulations relating to "financial products and services," which are broadly defined in the Financial Services Law to mean essentially any product or service offered by a Department-regulated entity. Accordingly, the Department has ample authority to adopt the proposed rule.

Other statutory authority includes: FSL Sections 202 and 408.

2. Legislative Objectives: The Financial Services Law is intended to ensure the safe and sound operation of the financial system. Cybercriminals present an ever-growing threat to that system. They can cause significant financial losses for Department-regulated entities and for New York consumers who use the products and services of those entities. In addition, the private information of such consumers may be revealed and/or stolen by cybercriminals for illicit purposes. The proposed rule is intended to ensure that all financial services providers regulated by the Department have and maintain cybersecurity programs that meet certain minimum cybersecurity standards in order to protect consumers and continue operating in a safe and sound manner.

3. Needs and Benefits: The proposed rule is necessary to ensure that Department-regulated entities are effectively addressing ever-growing cybersecurity risks in order to protect consumers and continue operating in a safe and sound manner.

4. Costs: All Department-regulated entities will be responsible for ensuring that they are in compliance with the proposed rule, which will impose some costs on their operations. The proposed rule provides for a limited exemption for certain smaller entities, based on each entity's number of employees, gross annual revenue, or year-end total assets. Entities that qualify for this limited exemption will be required to comply with only a limited number of sections in the proposed rule; thus, the costs of compliance for such entities is likely to be lower.

It is also anticipated that the costs of compliance will be offset to varying degrees when, as a result of complying with the proposed rule, entities avoid or mitigate cyber attacks that might otherwise have caused financial and other losses.

There should be no costs to any local governments as a result of the proposed rule.

5. Local Government Mandates: The proposed amendments do not impose any new programs, services, duties or responsibilities on local government.

6. Paperwork: The proposed rule requires entities to maintain a written cybersecurity policy and other written cybersecurity procedures and plans; to develop cybersecurity reports for presentation to the entity's board or a senior officer; to submit to the superintendent an annual certification of compliance with the proposed rule; and to keep books and records documenting compliance.

Entities that qualify for the limited exemption have fewer written policy and record-keeping requirements.

7. Duplication: Part 421 of Title 11 of the New York Codes, Rules and Regulations, promulgated in conformance with the federal Gramm-Leach-Bliley Act, requires insurance entities to implement a comprehensive written information security program. To a very limited extent, the proposed rule overlaps with Part 421, but the proposed rule includes requirements that are far more specific than Part 421 in order to achieve more robust cybersecurity coverage and to ensure that the Department's regulated entities have and maintain cybersecurity programs that meet certain minimum cybersecurity standards in order to protect consumers and continue operating in a safe and sound manner. Notably, Section 6807(b) of the Gramm-Leach-Bliley Act allows states to implement a statute, regulation, order, or interpretation affording protections that are greater than those listed in the Gramm-Leach-Bliley Act.

8. Alternatives: None.

9. Federal Standards: As noted earlier, see "Duplication," above, the proposed rule will, in some respects, exceed minimum standards established by the federal Gramm-Leach-Bliley Act. The Department believes that the proposed rule is not inconsistent with the federal Gramm-Leach-Bliley Act. Indeed, the proposed rule includes requirements that are more specific than those in the federal Gramm-Leach-Bliley Act in order to achieve more robust cybersecurity coverage and to ensure that the Department's regulated entities protect consumers and continue operating in a safe and sound manner. Section 6807(b) of the Gramm-Leach-Bliley Act allows states to implement a statute, regulation, order, or interpretation affording protections that are greater than those listed in the Gramm-Leach-Bliley Act.

10. Compliance Schedule: Regulated entities will have 180 days from the effective date of the proposed rule to comply with its requirements, except as otherwise specified. The proposed rule will be effective March 1, 2017. Covered Entities will be required to annually prepare and submit to the Superintendent a certification of compliance under Section 500.17 commencing February 15, 2018.

Revised Regulatory Flexibility Analysis

1. Effect of the Rule: The proposed rule applies to all Department-regulated entities, but certain small businesses may qualify for a limited exemption provided for in Section 500.19 of the proposed rule. Those entities that qualify for the limited exemption – those that fall below the minimum specified number of employees, gross annual revenue, or year-end total assets – shall be exempt from the requirements of the proposed rule other than the requirements enumerated in Section 500.19.

The proposed rule does not apply to local governments and will not impose any adverse economic impact or any reporting, recordkeeping or other compliance requirements on local governments.

2. Compliance Requirements: Small businesses that do not qualify for the limited exemption found in Section 500.19 will be subject to all of the requirements of the proposed rule. If a small business does qualify for the limited exemption, such small business will be exempt from Sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of the proposed rule.

3. Professional Services: A small business will not necessarily need any professional services to comply with the proposed rule. However, under the proposed rule, a Department-regulated entity that is a small business (or any other Department-regulated entity) that does not qualify for the limited exemption under Section 500.19 may use a third party service provider as its Chief Information Security Officer.

The proposed rule does not apply to local governments.

4. Compliance Costs: Like all businesses subject to the proposed rule, small businesses will be responsible for ensuring that they are in compliance with the proposed rule, which will impose some costs on their operations. The Department believes that the need for compliance outweighs such costs.

5. Economic and Technological Feasibility: The Department believes it will be economically and technologically feasible for small businesses to comply with the requirements of the proposed rule.

6. Minimizing Adverse Impacts: To minimize any adverse economic impact of the proposed rule on small businesses, the Department has included the limited exemption for smaller entities (Section 500.19 of the proposed rule). If a small businesses qualifies for the limited exemption, it will be subject to fewer compliance requirements.

7. Small Business and Local Government Participation: The proposed rule will be published publicly, including on the Department's website, for notice and comment, which will provide small businesses with the opportunity to participate in the rule making process.

The proposed rule does not impact local governments.

Revised Rural Area Flexibility Analysis

A revised Rural Area Flexibility Analysis (RAFA) is not required because the revisions to the proposed regulation do not change the conclusions set forth in the previously published RAFA.

Revised Job Impact Statement

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.

Assessment of Public Comment

The New York State Department of Financial Services (the "Department" or "DFS") received over 150 comments on proposed rule 23 NYCRR 500 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. These comments are summarized as follows.

Many commentators commended the Department for its efforts in addressing cybersecurity. Some commentators suggested that DFS expand or heighten the proposed regulation's requirements by, for example, setting a time limit within which Covered Entities would be required to have identified a breach; requiring Covered Entities to perform more testing of their systems and to retain outside consultants for testing; and mandating additional cybersecurity measures. DFS believes that the proposed regulation effectively addresses the required elements of a cybersecurity program at this time, along with DFS's overall supervisory authority.

A number of commentators supported the proposal's goal to set minimum standards for cybersecurity practices, so that cybersecurity programs match the relevant risks and keep pace with technological advances. Commentators asserted that provisions in the regulation should be made more flexible and risk-based. DFS has clarified in the revised regulation that certain requirements are linked to the results of the Covered Entity's Risk Assessment, consistently with the proposal's original stated intent. To be clear, the Department believes that each Covered Entity should model its cybersecurity program on the Covered Entity's cybersecurity risks, but the Risk Assessment is not intended to permit a cost-benefit analysis of acceptable losses where an institution is faced with cybersecurity risks.

Commentators requested clarification, tailoring and/or narrowing of certain definitions, including the following:

Cybersecurity Event: Some commentators stated that this definition, and particularly its use of words like "unsuccessful" and "attempt," was overbroad and resulted in overbroad requirements. DFS has not revised this definition because it is important for a comprehensive cybersecurity program to address attempts even where unsuccessful. However, the Department has revised several of the provisions of specific concern by requiring that certain provisions be based on the Risk Assessment and by including materiality qualifiers, such as in the Notices to Superintendent section.

Information System: Some commentators stated that this definition is overbroad and resulted in overbroad requirements. The Department has not revised this definition because the Department believes its scope is appropriate in the context of the revised proposed regulation.

Nonpublic Information: Commentators variously asserted that this definition is overbroad or unclear, or argued that it should more closely track the language of other standards in order to, for example, reduce the need for entities to classify data in multiple ways when attempting to meet the requirements of different regulations or laws. The Department has made several revisions to this definition in response to these comments.

Publicly Available Information: Some commentators asserted that this definition is too narrow and should encompass more information, or should otherwise be revised. The Department has not revised this definition because the Department believes it is appropriate in the context of the revised proposed regulation.

Some commentators questioned the use of the term Chief Information Security Officer ("CISO") – specifically, that the regulation might require hiring or appointing an individual whose exclusive job would be to serve as a CISO under that specific title. In response, DFS has revised section 500.04 to clarify that each Covered Entity shall designate a qualified individual to perform the functions of a CISO, but that DFS is not requiring a specific title, or an individual exclusively dedicated to CISO activity.

Commentators asserted that a variety of other specific provisions were overly prescriptive and/or insufficiently tied to the results of the Risk Assessment. In many cases, commentators suggested specific alternative language to address such issues. The Department has revised the Risk As-

sessment section (500.09) and other sections to clarify and/or make more explicit the Department's original intent to have risk-based requirements tied to the Covered Entity's Risk Assessment as provided in the overall regulation and the Department's supervisory authority. Risk Assessment is now a defined term. In addition, revisions have been made to the following sections: Cybersecurity Program (500.02), Cybersecurity Policy (500.03), Penetration Testing and Vulnerability Assessments (500.05), Access Privileges (500.07), Multi-Factor Authentication (500.12), and Encryption of Nonpublic Information (500.15).

Some commentators stated that requirements in the Cybersecurity Personnel and Intelligence section (500.10) and the Training and Monitoring section (500.14) should be more risk-based. In response, the Department revised these sections to, among other things, more specifically tailor certain requirements.

Some commentators 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 commentators claimed that the six-year retention period was too long. In response, the Department has made certain revisions to section 500.06, including amending section 500.06(a) to be explicitly based on the Risk Assessment and decreasing the retention period in section 500.06(b) to five years.

A number of commentators expressed concerns that the Limitations on Data Retention section (500.13) does not sufficiently take into account certain legitimate business reasons for which data might be retained. The Department has revised section 500.13 to explicitly take into account circumstances where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

Commentators also stated that the requirements in section 500.11 regarding third parties doing business with a Covered Entity were too prescriptive, especially the preferred contract provisions. Commentators also expressed concerns that many Covered Entities would have difficulty complying because they would not have sufficient leverage over third parties to effect some of the proposal's requirements. In addition, commentators expressed concern that the required annual assessment for all third party service providers would be burdensome, given the large number of third party service providers used by some Covered Entities. The Department has amended this section so that its requirements are more explicitly based on the Covered Entity's Risk Assessment. In addition, DFS has eliminated a provision in section 500.11(b) that may have unintentionally suggested that Covered Entities are required to audit the systems of all third party service providers. Also, in response to comments seeking greater clarity in regard to the requirements of this section, the Department has added a defined term, "Third Party Service Provider(s)."

Commentators claimed that the proposal includes overly broad reporting requirements that would result in many reports that are of little cybersecurity value. Additionally, commentators claimed that a 72-hour reporting timeframe is too short. Some commentators noted, for example, that in the first few days of a Cybersecurity Event, the entity is still gathering information on what happened. Also, commentators expressed concern about the confidentiality of notices provided to the Department. Based on its experience, the Department believes that the 72-hour reporting timeframe is essential to protect the markets while the Department does not intend for the reporting to include unnecessary information. Accordingly, the Department has revised section 500.17 to state that notice is required within 72 hours of a determination that a Cybersecurity Event as follows has occurred: (1) Cybersecurity Events of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body, and (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity. In addition, DFS has added a confidentiality section to the proposed regulation.

Some commentators asserted that the annual certification requirement of section 500.17(b) should be eliminated. They argued, for example, that the annual certification requirement is unnecessary, or that compliance with the requirement would be costly and divert resources from other uses. Other commentators sought revisions in the annual certification requirement and/or certification form. The Department has determined that the annual certification is an important part of the regulation and the Department's oversight of the financial market. The Department does not believe that the requirement creates unnecessary burdens; to the contrary, the Department believes the process is essential to good corporate governance. Accordingly, the Department has retained the annual certification requirement and the certification form included as Appendix A. In addition, the Department has determined that the content of the certification form and certification requirement are appropriate in the context of the revised proposed regulation.

Certain entities requested exemptions, but the Department determined not to alter the definition of Covered Entities, which in the Department's view provides adequate guidance as to which entities are covered. Some businesses, including small businesses, expressed concerns regarding cost and burden. The Department has included in the revised proposal several exemptions based on the risk that particular entities or circumstances present:

- The Department has included a limited exemption for a Covered Entity that does not directly or indirectly operate, maintain, utilize or control any Information Systems, and that does not control, generate, receive or possess Nonpublic Information.
- The Department has included an exemption for an employee, agent, representative, designee or Affiliate of a Covered Entity, who is itself a Covered Entity, to the extent that the employee, agent, representative, designee or Affiliate is covered by the cybersecurity program of the Covered Entity.
- The Department has amended the limited exemption in section 500.19(a) by adding Covered Entities with fewer than 10 employees including independent contractors, deleting Covered Entities with fewer than 1000 customers in each of the last three calendar years, and changing "and" to "or" in two locations.

The Department has also added a notice of exemption filing requirement for entities claiming an exemption.

Multiple commentators expressed concern about the implementation timeframes. The Department has added to the Transitional Periods section of the revised proposal (500.22) a number of additional transitional periods. These additional transitional periods are designed to provide outside deadlines for compliance with specific requirements, while urging Covered Entities to comply as soon as possible in order to protect customer data.

Some commentators asserted that the proposed regulation should harmonize more closely with other standards, including state, federal and international standards, both existing and proposed. The Department has been continually mindful of other standards and approaches and believes that the revised regulation is appropriately consistent with the goal of setting minimum standards.

Several commentators stated that all minimum standards should be eliminated and the Department should either (1) release guidance rather than promulgate a regulation or (2) wait for the federal government to promulgate regulations. The Department has not accepted any such suggestions, as the Department continues to believe that it should promptly promulgate a cybersecurity regulation as time is of the essence regarding cybersecurity protections. For similar reasons, no revisions have been made by the Department in response to comments that Covered Entities should be allowed to develop their own risk based controls, or otherwise follow other standards, in lieu of meeting the regulation's requirements.

New York State Gaming Commission

NOTICE OF ADOPTION

Require Thoroughbred Horse Trainers to Complete Four Hours of Continuing Education Each Year

I.D. No. SGC-37-16-00007-A
Filing No. 1150
Filing Date: 2016-12-13
Effective Date: 2016-12-28

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

Action taken: Amendment of section 4002.8 of Title 9 NYCRR.

Statutory authority: Racing, Pari-Mutuel Wagering and Breeding Law, sections 103(2), 104(1) and (19)

Subject: Require thoroughbred horse trainers to complete four hours of continuing education each year.

Purpose: To preserve the integrity of pari-mutuel racing while generating reasonable revenue for the support of government.

Text or summary was published in the September 14, 2016 issue of the Register, I.D. No. SGC-37-16-00007-P.

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

Text of rule and any required statements and analyses may be obtained from: Kristen Buckley, New York State Gaming Commission, One Broadway Center, P.O. Box 7500, Schenectady, New York 12301, (518) 388-3407, email: gamingrules@gaming.ny.gov