(1) tracking key information for each asset, including, as applicable, the following:

(i) owner;

(ii) location;

(iii) classification or sensitivity;

(iv) support expiration date; and

(v) recovery time requirements.

(2) the frequency required to update and validate the covered entity's asset inventory.

(b) As part of its cybersecurity program, each covered entity shall include policies and procedures for the secure disposal on a periodic basis of any nonpublic information identified in section [500.1(g)(2)-(3)] 500.1(i)(2)-(3) of this Part that is no longer necessary for business operations or for other legitimate business purposes of the covered entity, except where such information is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained.

The title of Section 500.14 is amended to read as follows: [Training and monitoring] Monitoring and training.

Section 500.14 is amended to read as follows:

(a) As part of its cybersecurity program, each covered entity shall:

(1) implement risk-based policies, procedures and controls designed to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, nonpublic information by such authorized users; [and]

(2) monitor and filter emails to block malicious content from reaching authorized users; and

(3) provide regular cybersecurity awareness and phishing training, exercises, and simulations when appropriate for all personnel that is updated to reflect risks identified by the covered entity in its risk assessment.

(b) Class A companies shall implement, unless the CISO has approved in writing the use of reasonably equivalent or more secure controls or tools:

(1) an endpoint detection and response solution to monitor anomalous activity, including but not limited to lateral movement; and

DRAFT

(2) a solution that centralizes logging and security event alerting.

The title of Section 500.15 is amended to read as follows: [Encryption] Protection of nonpublic information.

Section 500.15 is amended to read as follows:

(a) As part of its cybersecurity program, [based on its risk assessment,] each covered entity shall implement [controls, including] a written policy requiring encryption[,] that meets industry standards to protect nonpublic information held or transmitted by the covered entity both in transit over external networks and at rest.

[(1) To the extent a covered entity determines that encryption of nonpublic information in transit over external networks is infeasible, the covered entity may instead secure such nonpublic information using effective alternative compensating controls reviewed and approved by the covered entity's CISO.]

[(2)] (b) To the extent a covered entity determines that encryption of nonpublic information at rest is infeasible, the covered entity may instead secure such nonpublic information using effective alternative compensating controls that have been reviewed and approved by the covered entity's CISO in writing. The feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.

[(b) To the extent that a covered entity is utilizing compensating controls under subdivision (a) of this section, the feasibility of encryption and effectiveness of the compensating controls shall be reviewed by the CISO at least annually.]

The title of Section 500.16 is amended to read as follows: [Incident response plan] Operational Resilience.

Section 500.16 is amended to read as follows:

(a) As part of its cybersecurity program, each covered entity shall establish [a] written [incident] plans that contain proactive measures to mitigate disruptive events and ensure operational resilience, including but not limited to incident response, business continuity, and disaster recovery plans.

(1) Incident response plan. Incident response [plan] plans shall be 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. Such plans shall address the following areas with respect to different types of cybersecurity events, including disruptive events such as ransomware incidents:

[(b) Such incident response plan shall address the following areas:

DRAFT

(1)] (i) the internal processes for responding to a cybersecurity event;

[(2)] (ii) the goals of the incident response plan;

[(3)] (iii) the definition of clear roles, responsibilities and levels of decision-making authority;

[(4)] (iv) external and internal communications and information sharing;

[(5)] (v) identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

[(6)] (vi) documentation and reporting regarding cybersecurity events and related incident response activities; [and]

[(7) the evaluation and revision as necessary of the incident response plan following a cybersecurity event] (vii) recovery from backups; and

(viii) updating the incident response plan as necessary.

(2) Business continuity and disaster recovery plan (for purposes of this Part, BCDR plan). BCDR plans shall be reasonably designed to ensure the availability and functionality of the covered entity's services and protect the covered entity's personnel, assets, and nonpublic information in the event of an emergency or other disruption to its normal business activities. Such plans shall, at minimum:

(i) identify documents, data, facilities, infrastructure, personnel, and competencies essential to the continued operations of the covered entity's business;

(ii) identify the supervisory personnel responsible for implementing each aspect of the BCDR plan;

(iii) include a plan to communicate with essential persons in the event of an emergency or other disruption to the operations of the covered entity, including employees, counterparties, regulatory authorities, third party service providers, disaster recovery specialists, the senor governing body, and any other persons essential to the recovery of documentation and data and the resumption of operations;

(iv) include procedures for the maintenance of back-up facilities, systems, and infrastructure as well as alternative staffing and other resources to enable the timely recovery of data and documentation and to resume operations as soon as reasonably possible following a disruption to normal business activities;

DRAFT

(v) include procedures for the back-up or copying, with sufficient frequency, of documents and data essential to the operations of the covered entity and storing of the information offsite; and

(vi) identify third parties that are necessary to the continued operations of the covered entity's business.

(b) Each covered entity shall distribute copies of the plans, and any revisions to them, to all relevant employees and shall maintain copies of the plans at one or more accessible offsite locations.

(c) Each covered entity shall provide relevant training to all employees responsible for implementing the plans regarding their roles and responsibilities.

(d) Each covered entity shall periodically test its:

(1) incident response plan with all staff critical to the response, including senior officers and the Chief Executive Officer (CEO), and shall revise the plan as necessary;

(2) BCDR plan with all staff critical to the continuity and response effort, including senior officers, and shall revise the plan as necessary; and

(3) ability to restore its systems from backups.

(e) Each covered entity shall maintain backups that are isolated from network connections.

Section 500.17 is amended to read as follows:

(a) Notice of cybersecurity event. Each covered entity shall notify the superintendent electronically in the form set forth on the department's website as promptly as possible but in no event later than 72 hours from a determination that a cybersecurity event has occurred that is [either] any of the following:

(1) cybersecurity events 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]

(2) cybersecurity events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity;

(3) cybersecurity events where an unauthorized user has gained access to a privileged account; or

(4) cybersecurity events that resulted in the deployment of ransomware within a material part of the covered entity's information system.

DRAFT

(b) Notice of compliance.

(1) Annually each covered entity shall submit to the superintendent electronically by April 15 either:

(i) a written [statement covering] certification which:

(*a*) certifies that, for the prior calendar year, [. This statement shall be submitted by April 15 in such form set forth as Appendix A of this Title, certifying that] the covered entity [is in compliance] complied with the requirements set forth in this Part[.]; and

(*b*) shall be based upon data and documentation sufficient to accurately determine and demonstrate such full compliance, including, to the extent necessary, documentation of officers, employees, representatives, outside vendors, and other individuals or entities, as well as other documentation, whether in the form of reports, certifications, schedules, or otherwise; or

(ii) a written acknowledgement which:

(*a*) acknowledges that, for the prior calendar year, the covered entity did not fully comply with all the requirements of this Part;

(*b*) identifies all provisions of this Part that the entity has not fully complied with and describes the nature and extent of such noncompliance; and

(*c*) identifies all areas, systems, and processes that require material improvement, updating, or redesign.

(2) Such certification or acknowledgement shall be submitted electronically in the form set forth on the department's website and shall be signed by the covered entity's CEO and its CISO. If the covered entity does not have a CISO, the certification or acknowledgment shall be signed by the CEO and by the senior officer responsible for the cybersecurity program of the covered entity.

(3) Each covered entity shall maintain for examination by the department all records, schedules and other documentation and data supporting [this certificate] the certification or acknowledgement for a period of five years. [To the extent a covered entity has identified] In the case of any acknowledgement, such supporting information shall thoroughly document the identification of, and the remedial efforts planned and underway to address, all areas, systems [or], and processes that require material improvement, updating or redesign, [the covered entity shall document the identification and the] and shall include a timeline for implementation of those remedial efforts [planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the superintendent].

DRAFT

(c) Notice and explanation of extortion payment. Each covered entity, in the event of an extortion payment made in connection with a cybersecurity event, shall provide the superintendent electronically, in the form set forth on the department's website, with the following:

(1) within 24 hours of the extortion payment, notice of the payment; and

(2) within 30 days of the extortion payment, 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.

Subdivisions (a), (e), (f) and (g) of Section 500.19 are amended to read as follows:

(a) Limited exemption. Each covered entity with:

(1) fewer than [10] 20 employees, including:

(i) employees and any independent contractors[,] of the covered entity [or its];

(ii) employees and any independent contractors of the covered entity's affiliates whose work is located in [New York or] this State; and

(iii) employees and any independent contractors of the covered entity's affiliates who are responsible for the business of the covered entity, regardless of their location;

(2) less than $5,000,000 in gross annual revenue in each of the last [3] three fiscal years from [New York] business operations of the covered entity and its affiliates in this State; or

(3) less than [$10,000,000] $15,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates, shall be exempt from the requirements of sections 500.4, 500.5, 500.6, 500.8, 500.10, 500.12, 500.14, 500.15 and 500.16 of this Part.

***

(e) A covered entity that qualifies for any of the above exemptions pursuant to this section shall file electronically a Notice of Exemption in the form set forth [as Appendix B of this Title] on the department's website within 30 days of the determination that the covered entity is exempt.

(f) The following persons are exempt from the requirements of this Part, provided such persons do not otherwise qualify as a covered entity for purposes of this Part: persons subject to

DRAFT

Insurance Law section 1110; persons subject to Insurance Law section 5904; [and] any accredited reinsurer, [or] certified reinsurer, or reciprocal jurisdiction reinsurer that has been [accredited or certified] so recognized pursuant to 11 NYCRR Part 125; individual insurance agents who are deemed to be inactive under Insurance Law section 2103; and individual licensees placed in inactive status under Banking Law section 599-i.

(g) In the event that a covered entity[, as of its most recent fiscal year end,] ceases to qualify for an exemption, such covered entity shall have [180] 120 days from [such fiscal year end] the date that it ceases to so qualify to comply with all applicable requirements of this Part.

Section 500.20 is amended to read as follows:

(a) This regulation will be enforced by the superintendent pursuant to, and is not intended to limit, the superintendent's authority under any applicable laws.

(b) The commission of a single act prohibited by this Part or the failure to act to satisfy an obligation required by this Part shall constitute a violation hereof. Such acts or failures include, without limitation:

(1) the failure to secure or prevent unauthorized access to an individual's or an entity's nonpublic information due to noncompliance with any section of this Part; or

(2) the failure to comply for any 24-hour period with any section or subsection of this Part.

(c) In assessing any penalty for a violation of this Part pursuant to the Banking Law, Insurance Law, or Financial Services Law, the superintendent may take into account, without limitation, factors including:

(1) the extent to which the covered entity has cooperated with the superintendent in the investigation of such acts;

(2) the good faith of the entity;

(3) whether the violations resulted from conduct that was unintentional or inadvertent, reckless, or intentional and deliberate;

(4) whether the violation was a result of failure to remedy previous examination matters requiring attention, or failing to adhere to any disciplinary letter, letter of instructions, or similar;

(5) any history of prior violations;

(6) whether the violation involved an isolated incident, repeat violations, systemic violations or a pattern of violations;

DRAFT

(7) whether the covered entity provided false or misleading information;

(8) the extent of harm to consumers;

(9) whether required, accurate, and timely disclosures were made to affected consumers;

(10) the gravity of the violations;

(11) the number of violations and the length of time over which they occurred;

(12) the extent, if any, to which the senior governing body participated therein;

(13) any penalty or sanction imposed by any other regulatory agency;

(14) the financial resources, net worth, and annual business volume of the covered entity and its affiliates; and

(15) such other matters as justice and the public interest require.

Section 500.21 is amended to read as follows:

(a) This Part will be effective March 1, 2017. Covered entities will be required to annually prepare and submit to the superintendent a certification of compliance with New York State Department of Financial Services Cybersecurity Regulations under section 500.17(b) of this Part commencing February 15, 2018.

(b) Amendments to this Part shall become effective upon publication of the Notice of Adoption in the State Register.

Subdivisions (c) and (d) are added to section 500.22 to read as follows:

(c) Covered entities shall have 180 days from the effective date of the amendments to this Part to comply with the new requirements set forth in this Part, except as otherwise specified.

(d) The following provisions shall include different transitional periods. Covered entities shall have:

(1) 30 days from the effective date of the amendments to comply with the new requirements specified in 500.17 of this Part; and

(2) one year from the effective date of the amendments to comply with the new requirements specified in 500.7(b), 500.12(c) and 500.14(b) of this Part.

A new Section 500.24 is added to read as follows:

500.24 Exemptions from electronic filing and submission requirements.

DRAFT

(a) A filer required to make an electronic filing or a submission pursuant to this Part may apply to the superintendent for an exemption from the requirement that the filing or submission be electronic by submitting a written request to the superintendent for approval at least 30 days before the filer shall submit to the superintendent the particular filing or submission that is the subject of the request.

(b) The request for an exemption shall:

(1) set forth the filer's DFS license number, NAIC number, Nationwide Multistate Licensing System number, or institution number;

(2) identify the specific filing or submission for which the filer is applying for the exemption;

(3) specify whether the filer is making the request for an exemption based upon undue hardship, impracticability, or good cause, and set forth a detailed explanation as to the reason that the superintendent should approve the request; and

(4) specify whether the request for an exemption extends to future filings or submissions, in addition to the specific filing or submission identified in paragraph (2) of this subdivision.

(c) The filer requesting an exemption shall submit, upon the superintendent's request, any additional information necessary for the superintendent to evaluate the filer's request for an exemption.

(d) The filer shall be exempt from the electronic filing or submission requirement upon the superintendent's written determination so exempting the filer, where the determination specifies the basis upon which the superintendent is granting the request and to which filings or submissions the exemption applies.

(e) If the superintendent approves a filer's request for an exemption from the electronic filing or submission requirement, then the filer shall make a filing or submission in a form and manner acceptable to the superintendent.

Appendices A and B to 23 NYCRR 500 are hereby repealed.

DRAFT