7/29/22

NEW YORK STATE
DEPARTMENT OF FINANCIAL SERVICES
PROPOSED
SECOND AMENDMENT TO 23 NYCRR 500

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

I, Adrienne A. Harris, Superintendent of Financial Services, pursuant to the authority granted by Sections 102, 201, 202, 301, 302, and 408 of the Financial Services Law, Sections 10, 14, 37(3), 37(4), and 44 of the Banking Law, and Sections 109, 301, 308, 309, 316, 1109, 1119, 1503(b), 1717(b), 2110, and 2127 and Articles 21 and 47 of the Insurance Law, do hereby promulgate the Second Amendment to Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York, to take effect upon publication of the Notice of Adoption in the State Register, to read as follows:

(NEW MATTER UNDERSCORED, DELETED MATTER IN BRACKETS)

Section 500.1 is amended to read as follows:

For purposes of this Part only, the following definitions shall apply:

(a) *Affiliate* means any person that controls, is controlled by or is under common control with another person. For purposes of this subdivision, *control* means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of a person, whether through the ownership of stock of such person or otherwise.

(b) *Authorized user* means any employee, contractor, agent or other person that participates in the business operations of a covered entity and is authorized to access and use any information systems and data of the covered entity.

(c) *Class A companies* mean those covered entities with:

(1) over 2,000 employees, including those of both the covered entity and all of its affiliates no matter where located; or

(2) over $1,000,000,000 in gross annual revenue averaged over the last three fiscal years from all business operations of the covered entity and all of its affiliates.

[(c)] (d) *Covered entity* means any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law, including entities that are also regulated by other government agencies.

[(d)] (e) *Cybersecurity event* means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system.

(f) *Independent audit* means an audit conducted by auditors free to make their decisions, not influenced by the covered entities being audited or by its owners, managers, and employees. Such an audit can be conducted by auditors internal or external to the covered entity and its affiliates.

[(e)] (g) *Information system* means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

[(f)] (h) *Multi-factor authentication* means authentication through verification of at least two of the following types of authentication factors:

(1) knowledge factors, such as a password;

(2) possession factors, such as a token[or text message on a mobile phone]; or

(3) inherence factors, such as a biometric characteristic.

[(g)] (i) *Nonpublic information* [shall mean] means all electronic information that is not publicly available information and is:

(1) business related information of a covered entity the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the covered entity;

(2) any information concerning an individual which because of name, number, personal mark, or other identifier can be used to identify such individual, in combination with any one or more of the following data elements:

(i) social security number;

(ii) drivers' license number or non-driver identification card number;

(iii) account number, credit or debit card number;

(iv) any security code, access code or password that would permit access to an individual's financial account; or

(v) biometric records;

(3) any information or data, except age or gender, in any form or medium created by or derived from a health care provider or an individual and that relates to:

(i) the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family;

(ii) the provision of health care to any individual; or

(iii) payment for the provision of health care to any individual.

[(h)] (j) *Penetration testing* means a [test] methodology [in which assessors attempt] for testing the security of information systems by attempting to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside the covered entity's information systems.

[(i)] (k) *Person* means any individual or [any non-governmental] entity, including but not limited to any [non-governmental] partnership, corporation, branch, agency or association.

(l) *Privileged account* means any authorized user account or service account that can be used to:

(1) perform security-relevant functions that ordinary users are not authorized to perform, including but not limited to the ability to add, change, or remove other accounts, or make configuration changes to operating systems or applications to make them more or less secure; or

(2) affect a material change to the technical or business operations of the covered entity.

[(j)] (m) *Publicly available information* means any information that a covered entity has a reasonable basis to believe is lawfully made available to the general public from: Federal, State or local government records; widely distributed media; or disclosures to the general public that are required to be made by Federal, State or local law.

[(1) For the purposes of this subdivision, a] A covered entity has a reasonable basis to believe that information is lawfully made available to the general public if the covered entity has taken steps to determine:

[(i)] (1) that the information is of the type that is available to the general public; and

[(ii)] (2) whether an individual can direct that the information not be made available to the general public and, if so, that such individual has not done so.

[(k)] (n) *Risk assessment* means the [risk assessment that each covered entity is required to conduct under section 500.9 of this Part] process of identifying cybersecurity risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, customers, consumers, other organizations, and critical infrastructure resulting from the operation of an information system. Risk assessments shall take into account the specific circumstances of the covered entity, including but not limited to its size, staffing, governance, businesses, services, products, operations, customers, counterparties, service providers, vendors, other relations and their locations, as well as the geographies and locations of

its operations and business relations. Risk assessments incorporate threat and vulnerability analyses, and consider mitigations provided by security controls planned or in place.

[(l)] (o) *Risk-based authentication* means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a person and requires additional verification of the person's identity when such deviations or changes are detected[, such as through the use of challenge questions].

(p) *Senior governing body* means the covered entity's board of directors (or an appropriate committee thereof) or equivalent governing body or, if neither of those exist, the senior officer of the covered entity responsible for the covered entity's cybersecurity program.

[(m)] (q) *Senior officer(s)* means the senior individual or individuals (acting collectively or as a committee) responsible for the management, operations, security, information systems, compliance and/or risk of a covered entity, including a branch or agency of a foreign banking organization subject to this Part.

[(n)] (r) *Third party service provider(s)* means a person that:

(1) is not an affiliate of the covered entity;

(2) provides services to the covered entity; and

(3) maintains, processes or otherwise is permitted access to nonpublic information through its provision of services to the covered entity.

Section 500.2 is amended to read as follows:

(a) [Cybersecurity program.] Each covered entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the covered entity's information systems and nonpublic information stored on those information systems.

(b) The cybersecurity program shall be based on the covered entity's risk assessment and designed to perform the following core cybersecurity functions:

(1) identify and assess internal and external cybersecurity risks that may threaten the security or integrity of nonpublic information stored on the covered entity's information systems;

(2) use defensive infrastructure and the implementation of policies and procedures to protect the covered entity's information systems, and the nonpublic information stored on those information systems, from unauthorized access, use or other malicious acts;

(3) detect cybersecurity events;

(4) respond to identified or detected cybersecurity events to mitigate any negative effects;

(5) recover from cybersecurity events and restore normal operations and services; and

(6) fulfill applicable regulatory reporting obligations.

(c) Class A companies shall conduct an independent audit of their cybersecurity programs at least annually.

[(c)] (d) A covered entity may meet the requirement(s) of this Part by adopting the relevant and applicable provisions of a cybersecurity program maintained by an affiliate, provided that such provisions satisfy the requirements of this Part, as applicable to the covered entity.

[(d)] (e) All documentation and information relevant to the covered entity's cybersecurity program, including the relevant and applicable provisions of a cybersecurity program maintained by an affiliate and adopted by the covered entity, shall be made available to the superintendent upon request.

Section 500.3 is amended to read as follows:

[Cybersecurity policy.] Each covered entity shall implement and maintain a written policy or policies, approved at least annually by [a senior officer or] the covered entity's senior governing body [board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the covered entity's policies and procedures] for the protection of its information systems and nonpublic information stored on those information systems. The policy or policies shall be implemented in accordance with documented procedures. The cybersecurity policy or policies and procedures shall be based on the covered entity's risk assessment and address, at a minimum, the following areas to the extent applicable to the covered entity's operations:

(a) information security;

(b) data governance and classification;

(c) asset inventory, [and] device management, and end of life management;

(d) access controls, including remote access, and identity management;

(e) business continuity and disaster recovery planning and resources;

(f) systems operations and availability concerns;

(g) systems and network security;

(h) systems and network monitoring;

(i) systems and application development and quality assurance;

(j) physical security and environmental controls;

(k) customer data privacy;

(l) vendor and third party service provider management;

(m) risk assessment; [and]

(n) incident response; and

(o) vulnerability and patch management.

The title of Section 500.4 is amended to read as follows: [Chief information security officer] Cybersecurity governance.

Section 500.4 is amended to read as follows:

(a) Chief information security officer. Each covered entity shall designate a qualified individual responsible for overseeing and implementing the covered entity's cybersecurity program and enforcing its cybersecurity policy (for purposes of this Part, chief information security officer or CISO). The CISO must have adequate independence and authority to ensure cybersecurity risks are appropriately managed. The CISO may be employed by the covered entity, one of its affiliates or a third party service provider. To the extent this requirement is met using a third party service provider or an affiliate, the covered entity shall:

(1) retain responsibility for compliance with this Part;

(2) designate a senior member of the covered entity's personnel responsible for direction and oversight of the third party service provider; and

(3) require the third party service provider to maintain a cybersecurity program that protects the covered entity in accordance with the requirements of this Part.

(b) Report. The CISO of each covered entity shall report in writing at least annually to the senior [covered entity's board of directors or equivalent] governing body. [If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer of the covered entity responsible for the covered entity's cybersecurity program.] The CISO shall report on the covered entity's cybersecurity program, plans for remediating inadequacies identified therein, and material cybersecurity risks. The CISO shall [consider] address in the written report to the extent applicable:

(1) the confidentiality of nonpublic information and the integrity and security of the covered entity's information systems;

(2) the covered entity's cybersecurity policies and procedures;

(3) material cybersecurity risks to the covered entity;

(4) overall effectiveness of the covered entity's cybersecurity program; and

(5) material cybersecurity events involving the covered entity during the time period addressed by the report.

(c) The CISO shall also timely report to the senior governing body regarding material cybersecurity issues, such as updates to the covered entity's risk assessment or major cyber events.

(d) If the covered entity has a board of directors, the board or an appropriate committee of the board shall require the covered entity's executive management or its delegates to develop, implement, and maintain the covered entity's information security program. The board or an appropriate committee of the board shall have sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge, to exercise effective oversight of cyber risk and a committee or subcommittee assigned responsibility for cybersecurity.

Section 500.5 is amended to read as follows:

The cybersecurity program for each covered entity shall 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:]

(a) [annual] Covered entities shall conduct:

(1) penetration testing of [the covered entity's] their information systems [determined each given year] by a qualified independent party based on relevant identified risks in accordance with the risk assessment at least annually; and

[(b) bi-annual] (2) regular vulnerability assessments, including [any] systematic scans or reviews of information systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the covered entity's information systems based on the risk assessment. Class A companies shall conduct systematic scans or reviews at least weekly.

(b) Covered entities shall ensure that material gaps found in testing are documented and reported to its senior governing body and senior management.

The title of Section 500.7 is amended to read as follows: Access privileges and management.

Section 500.7 is amended to read as follows:

(a) As part of its cybersecurity program, based on the covered entity's risk assessment each covered entity shall:

(1) limit user access privileges to information systems that provide access to nonpublic information [and shall periodically review such access privileges] to those necessary to perform the user's job;

(2) limit the number of privileged accounts and limit the access functions of privileged accounts to only those necessary to perform the user's job;

(3) limit the use of privileged accounts to only when performing functions requiring the use of such access;

(4) periodically review all user access privileges and remove accounts and access that are no longer necessary; and

(5) disable or securely configure all protocols that permit remote control of devices.

(b) To the extent passwords are employed as a method of authentication, the covered entity shall ensure strong, unique passwords are used. Class A companies shall also monitor privileged access activity and, unless the covered entity's CISO approves in writing the use of reasonably equivalent or more secure access controls, shall implement:

(1) a password vaulting solution for privileged accounts; and

(2) an automated method of blocking commonly used passwords.

Subdivision 500.8(b) is amended to read as follows:

(b) All such procedures, guidelines and standards shall be [periodically] reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the covered entity at least annually.

Subdivisions 500.9(c) and (d) are added to Section 500.9 to read as follows:

(c) The risk assessment shall be updated at least annually. The covered entity also shall conduct an impact assessment whenever a change in the business or technology causes a material change to the covered entity's cyber risk.

(d) Class A companies shall use external experts to conduct a risk assessment at least once every three years.

Section 500.10 is amended to read as follows:

(a) [Cybersecurity personnel and intelligence.] In addition to the requirements set forth in section 500.4(a) of this Part, each covered entity shall:

(1) utilize qualified cybersecurity personnel of the covered entity, an affiliate or a third party service provider sufficient to manage the covered entity's cybersecurity risks and to perform or oversee the performance of the core cybersecurity functions specified in section 500.2(b)(1)-(6) of this Part;

(2) provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks; and

(3) verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures.

(b) A covered entity may choose to utilize an affiliate or qualified third party service provider to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in [section] sections 500.4 and 500.11 of this Part.

Section 500.11 is amended to read as follows:

(a) [Third party service provider policy.] Each covered entity shall implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third party service providers. Such policies and procedures shall be based on the risk assessment of the covered entity and shall address to the extent applicable:

(1) the identification and risk assessment of third party service providers;

(2) minimum cybersecurity practices required to be met by such third party service providers in order for them to do business with the covered entity;

(3) due diligence processes used to evaluate the adequacy of cybersecurity practices of such third party service providers; and

(4) periodic assessment of such third party service providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(b) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to third party service providers including to the extent applicable guidelines addressing:

(1) the third party service provider's policies and procedures for access controls, including its use of multi-factor authentication as required by section 500.12 of this Part, to limit access to relevant information systems and nonpublic information;

(2) the third party service provider's policies and procedures for use of encryption as required by section 500.15 of this Part to protect nonpublic information in transit and at rest;

(3) notice to be provided to the covered entity in the event of a cybersecurity event directly impacting the covered entity's information systems or the covered entity's nonpublic information being held by the third party service provider; and

(4) representations and warranties addressing the third party service provider's cybersecurity policies and procedures that relate to the security of the covered entity's information systems or nonpublic information.

[(c) Limited exception. An agent, employee, representative or designee of a covered entity who is itself a covered entity need not develop its own third party information security policy pursuant to this section if the agent, employee, representative or designee follows the policy of the covered entity that is required to comply with this Part.]

Section 500.12 is amended to read as follows:

(a) [Multi-factor authentication.] Based on its risk assessment, each covered entity shall use effective controls, which may include multi-factor authentication or risk-based authentication, to protect against unauthorized access to nonpublic information or information systems.

(b) Multi-factor authentication shall be utilized 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] remote access to the network and enterprise and third-party applications from which nonpublic information is accessible.

(c) Multi-factor authentication shall be utilized for all privileged accounts, except for service accounts:

(1) that prohibit interactive log in; and

(2) the covered entity's CISO has approved in writing the implementation of compensating controls that achieve reasonably equivalent security.

The title of Section 500.13 is amended to read as follows: [Limitations on] Asset and data retention management.

Section 500.13 is amended to read as follows:

(a) As part of its cybersecurity program, each covered entity shall implement written policies and procedures designed to ensure a complete, accurate, and documented asset inventory, including, all information systems and their components such as hardware, operating systems, applications, infrastructure devices, APIs, and cloud services. The asset inventory shall be maintained in accordance with written policies and procedures. At a minimum, such policies and procedures shall include:

(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

(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:

(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;

(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.

(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].

(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

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;

(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.

(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.