SQUIRE PATTON BOGGS

New York is Raising the Cybersecurity Bar[i]

This article was published in Thomson Reuters' FinTech Law Report: E-Banking, Payments and Commerce in the Mobile World in the September/October 2017 issue.

Not just another high-level, non-binding cybersecurity recommendation

Over the past couple years, entities operating in the U.S. have been inundated with a patchwork of state and federally-enforceable regulations as well as non-binding "guidelines" or "recommendations". Under existing law in a handful of states, organizations are required to secure personal information for in-state residents, while other states require to ensure the security of any personal information, including that of non-residents. [ii]

In the financial services sector, the developing body of enforceable regulations have centered around mandating sufficient security measures to protect personal financial information, transaction data, and funds.[iii] Federal and state agencies, trade associations and professional organizations have also taken it upon themselves to publish their own respective cybersecurity guidelines.

In general, many of today's cybersecurity requirements are unenforceable and high-level, suggesting, for example, that an entity develop a cybersecurity program to "protect data" or "respond to incidents in a timely manner." While high-level regulations (or non-binding recommendations) afford organizations wide latitude to develop cybersecurity programs, organizations also struggle to determine with confidence whether their programs expose them to regulatory risk.

New York Department of Financial Services Cybersecurity Rule (23 NYCRR 500)

Entering the fray of cybersecurity regulation, the New York Department of Financial Services (NYDFS) issued new cybersecurity rules for licensed entities. The NYDFS passed a cybersecurity rule –23 NYCRR 500 ("Part 500") – applicable to most banks, financial services entities and insurance entities licensed by the state[iv], subject to certain exemptions.[v] [vi] The regulations under this rule surpass the basic requirements under existing state cybersecurity statutes. [vii] Organizations governed by this state agency must now develop strong cybersecurity programs and implement specific security controls, policies and procedures to protect their information .

Unlike most state data security and breach notification laws[viii], which protect consumers' personal information, Part 500 aims to protect both information systems and the non-public information (NPI) stored on them. The rule's own introduction explicitly requires organizations to create a "robust" cybersecurity program based on its own unique risk profile, requiring senior management to "take this issue seriously," and requiring each entity to file annual compliance certifications with the Superintendent.[ix]

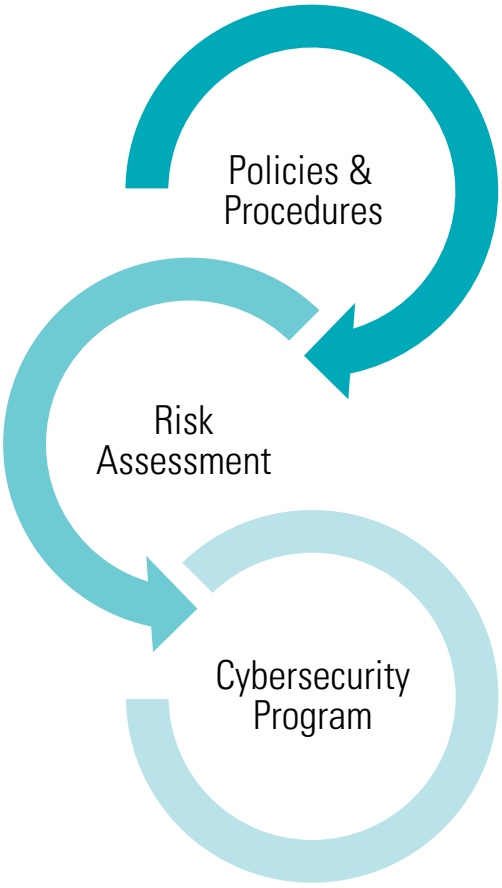
The Department's language signals a requirement that every entity should re-evaluate its programs and identify areas that require improvement (even entities with existing, possibly mature, cybersecurity programs) in order to comply with Part 500, due to the fact that strong cybersecurity protection in the insurance, banking and financial services industry is a stated "priority for New York State."[x]

Part 500 does not create novel mechanisms for protecting information and systems. Rather, it reflects accepted practices in the information security industry. The baseline it prescribes for regulated entities raises the bar from existing state data security statutes, regulations, and high-level (non-binding) guidelines.

Regulated entities with existing strong cybersecurity programs can likely make a handful of minor adjustments in order to comply. Refer to the following sections for a detailed break-down of the three main components required to comply with the obligations imposed by Part 500.

New York's Part 500: Raising the Cybersecurity Bar

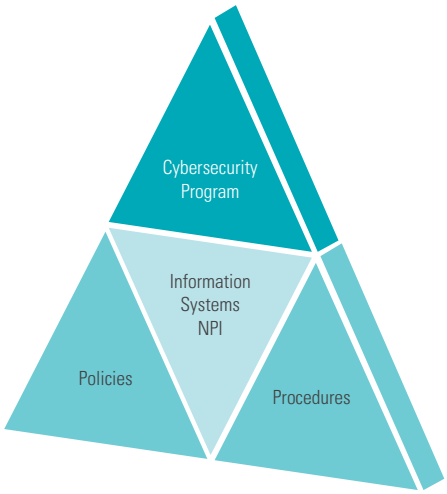
Three Main Components



Part 500 comprises 23 subsections, which describe entities' cybersecurity obligations. Most, if not all, of the obligations can be categorized into three main components: a Cybersecurity Program, Policies and Procedures, and a Risk Assessment of Information Systems. Each are based on one another and also inform one another.

	Goal	Must Be Based On
Cybersecurity Program	Protect Information Systems and the NPI stored on them[xi]	Risk Assessment[xii]
Policies & Procedures		
Risk Assessment	Inform the Cybersecurity Program's design[xiii]	Policies & Procedures[xiv]

The Cybersecurity Program and Policies & Procedures protect the entity's Information Systems and the NPI stored thereon.



The following sections addresses what Part 500 requires for each of its three main components, followed by a discussion of the remaining requirements under the rule.

Policies and Procedures[xv]

Part 500 requires an organization to maintain written policies and procedures that are based on the Risk Assessment and designed to protect information systems and the information stored thereon. The policies and procedures must be approved by a Senior Officer of the organization or the Board of Directors, designated Board committee, or equivalent body.[xvi] Note that for the required annual certifications, it is the Board of Directors who must attest to compliance with Part 500.[xvii] A Board subcommittee may not.[xviii]

Although seemingly negligible, the requirement that policies and procedures must be *written* should not be overlooked. Federal regulators consistently determine that proper cybersecurity programs must be written and often draft consent decrees to require an organization to create and maintain *written* cybersecurity policies and procedures.[xix] If a financial services organization has a mature cybersecurity program, its policies and procedures are likely written. However, those should still need to be compared against the specific requirements in Part 500 to ensure compliance. In addition to the general requirement that policies and procedures be written, Part 500 separately requires four of the above categories to be written.

Policies and procedures must include detailed instructions for carrying out a Risk Assessment[xx] and address how consumers will be notified in the aftermath of a data breach[xxi], as well as the following components of a cybersecurity program:

(a) information security; (b) data governance and classification; (c) asset inventory and device management; (d) access controls 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.[xxii]

Part 500 includes more granular requirements for certain categories, discussed below, including: access controls, systems and network monitoring, application development, Third Party Service Provider management, risk assessment and incident response.

- Organizations therefore need to account for, update, revise and produce policies and procedures. Although not required, organizations could consider cataloging policies and procedures to increase efficiency with reviews, updates and any Superintendent requests.

Risk Assessment

The goal of an entity's Risk Assessment, as required by Part 500, is to inform the design of the Cybersecurity Program[xxiii] and for it to be carried out according to the policies and procedures[xxiv]. The Risk Assessment must be documented and updated as reasonably necessary to address changes specific to the entity itself, in information systems, NPI or business operations.[xxv] When an organization creates instructions for its Risk Assessment, it should do so with an eye towards creating repeatable processes that avoid heavy lifting each year. For example, as the entity experiences changes, certain parts of the Cybersecurity Program and policies and procedures may necessitate revision. The instructions for conducting the Risk Assessment could include a checklist of items that potentially could have changed (i.e., technological developments, evolving threats, particular cybersecurity risks of business operations, types or quantities of NPI collected or stored, availability and effectiveness of controls to protect NPI and information systems)[xxvi] along with the correlating sections of the Cybersecurity Program or policies and procedures that might require revision as a result of any such changes. This could reduce the work involved in identifying required revisions under Part 500. Part 500 also requires that information security personnel continue to stay up to date on evolving threats.[xxvii] Since the Risk Assessment requires similar efforts, the two could be combined for efficiency.

In its subsequently-published FAQs, the Department stressed that analyzing threats – including unsuccessful threats or attacks – is an important factor in continually evaluating and improving cybersecurity programs, urging organizations to not only identify threats on an ongoing basis, but to identify potential improvements to their threat assessment programs as well.[xxviii]

Risk Assessment Required Components

The Risk Assessment must include:

- Criteria to evaluate and categorize identified risks or threats to the organization.[xxix]

Threats and risks could be categorized, for example, into external risks and threats to the entity, internal risks and threats to the entity and third-party incidents that could impact the entity.

Each sector and organization within a sector may have different criteria for evaluating threats and risks. For example, two insurance carriers may assess the risks associated with independent contractor claims agents with remote access to the company's systems from their home computers if one carrier requires extra authentication (multi-factor authentication) for remote access and the other has security measures in place to restrict claims agents from viewing other agents' customer data. Both would need to evaluate the risk of an administrator accidentally granting the agents' accounts broader access to customer data than intended. Only the latter scenario runs the risk that a claims agent who uses an easily-guessable password can be a weak link for a malicious party gaining remote access to company systems (i.e., without having to use a second factor beyond the guessed password in order to authenticate to the company's servers).

Risks and vulnerabilities identified during the Risk Assessment should be provided to the security personnel in charge of annual penetration test and bi-annual vulnerability assessments to ensure their adequacy.

- Criteria for assessing whether existing controls are sufficient to ensure confidentiality, integrity, security and availability of information systems and NPI, particularly in light of threats and risks identified.
- Requirements for mitigating or accepting risks based on the Risk Assessment and how to address the risks in the Cybersecurity Program.

Many risks cannot be eliminated but can be mitigated. The organization should establish criteria for determining whether a risk is acceptable to the enterprise or not, and should prescribe changes to the Cybersecurity Program that can address the risk going forward (such as adding multi-factor authentication for remote access). Since threats and attack techniques evolve, the risk of a particular threat may be negligible for several years and become serious in subsequent years. Several years ago, a sizable portion of organizations dismissed security professionals' warnings of the possibility of ransomware attacks bringing entire enterprises to a halt for days, and the need to create emergency backup plans. Now that ransomware has become increasingly prevalent and damaging, organizations may choose to implement measures in their Cybersecurity Programs to reduce the risk of business operations coming to a halt from a ransomware attack.

Cybersecurity Program

The goal of a regulated entities' Cybersecurity Program is to protect the "confidentiality, integrity and availability"[xxx] of information systems and the NPI residing thereon[xxxi], and must be based on the Risk Assessment.[xxxii] The Risk Assessment should drive revisions to the entity's security controls in response to changes in the entity's environment.[xxxiii] A NYDFS FAQ issued after the rule added that the Cybersecurity Program must address consumer data privacy and other consumer protection issues.[xxxiv]

Importantly, the information relevant to an entity's Cybersecurity Program must be disclosed to the Superintendent upon request[xxxv]. Organizations should make employees aware of the fact that information might be disclosed to the Superintendent, and that employees should therefore take that into consideration when creating documentation.

6 Core Functions of the Cybersecurity Program

The Cybersecurity Program must include each of six core functions along with additional components. We have identified and categorized the requirements from the entire rule under each core function. Each action item below corresponds to a particular requirement in the regulation. By progressing through these functions systematically, organizations can streamline the process of ensuring compliance with the broader set of requirements in Part 500.

Core Function 1: Identify and assess internal and external threats to the security or integrity of NPI stored on information systems[xxxvi]

Action Items	Reference
Identify internal[xxxvii] threats to secu[xxxviii]rity of NPI	500.02(b)(1)
Identify external threats to security of NPI	500.02(b)(1[xxxix])
Identify internal th[xl]reats to integrity of NPI	500.02(b)(1)
Identify external threats to integrity of NPI	500.02(b)(1)
Assess all of the above	500.02(b)(1), 500.09(b)(1)
Categorize identified risks and threats	500.09(b)(1)

Core Function 2: Use defensive infrastructure and the implementation of policies and procedures to protect information systems and the NPI stored thereon from unauthorized access, use or other malicious acts[xli]

Action Items	Reference
Ensure defensive infrastructure designed to prevent unauthorized access, use or other malicious acts	500.02(b)(2)
Ensure policies and procedures are designed to prevent unauthorized access, use or other malicious acts	500.02(b)(2)
Limit user access privileges to information systems that *provide access to* NPI	500.07
Periodically review access privileges	500.07
Assess whether controls adequately protect the confidentiality, integrity, security and availability of information systems and NPI in the context of identified risks	500.09(b)(2)

Core Function 3: Detect Cybersecurity Events[xlii], which are any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored thereon[xliii]

Action Items	Reference
Develop list of possible events	
Identify how each possible event can be detected using existing means	
Identify other means necessary to be procured	
Ensure audit trails are sufficient to detect and respond to unwanted acts that have a reasonable likelihood of materially harming any material part of normal operations	500.06(a)(2)
Retain such audit trails for 3 years	500.06(b)

Core Function 4: Respond to identified or detected Cybersecurity Events to mitigate any negative effects[xliv]

Action Items	Reference
Retrieve list of risks identified through Risk Assessment and develop plan to address according to policies and procedures	500.09(b)(3)
Develop plan for how to address Cybersecurity Events	500.02(4)
Follow relevant policies and procedures	500.03 (a) – (n)

Core Function 5: Recover from Cybersecurity Events and restore normal operations and services[xlv]

Action Items	Reference
Follow relevant policies and procedures	500.03(e), (f)
Securely maintain systems based on Risk Assessment such that material financial transactions can be reconstructed sufficiently to support normal operations and obligations	500.06(a)(1)
Retain such records for five years	500.06(b)

Core Function 6: Fulfill applicable regulatory reporting obligations[xlvi]

Action Items	Reference
Identify all regulatory reporting requirements (outside Part 500)	500.02(b)(6)
Report to other regulatory authorities as required	
Notify NYDFS Superintendent within 72 hours following determination of obligation to report under another regulation	500.17(a)(1)
Notify NYDFS Superintendent within 72 hours of determining a Cybersecurity Event has a reasonable likelihood of materially harming a material part of normal operations, including harm to consumers	500.17(a)(2), FAQ #9
Submit annual certification to Superintendent affirming that the Board of Directors has, by Resolution,[xlvii] reviewed appropriate documentation and determined that the entity complies with Part 500	500.17(b), Appendix A
Maintain for examination by NYDFS all records, schedules and data supporting annual certification for 5 years	500.17(b)

Additional Cybersecurity Program Components

Scattered throughout Part 500, NYDFS imposes discrete requirements that can be considered additional components of a compliant Cybersecurity Program under the rule. While these could be categorized under the six core functions, they warrant separate attention so that they can be properly understood.

Technical Requirements

Encryption

Part 500 is one of the country's first regulations to mandate encryption – here, for NPI at rest (stored on computers, servers, in the cloud or on other devices) and in transit (being sent via email or other transmission method). [xlviii] The rule leaves room for the Chief Information Security Officer to allow an equally protective security measure to be used in place of encryption. [xlix] If the CISO does so, however, this exception must be reviewed annually to determine whether, under the Risk Assessment, the risk of not encrypting NPI continues to be sufficiently mitigated.[l]

Monitoring

The entity must establish risk-based policies, procedures and controls to monitor authorized user's activities to detect unauthorized use or tampering with NPI (i.e. insider threats)[li]. This requirement should help organizations avoid focusing exclusively on defending against intrusions to the outer perimeter of their network. Increasingly, attackers gain control of legitimate users' devices and when the user connects to his or her corporate network, the attacker is already inside the network, never having penetrated the outer perimeter.

Penetration Tests and Vulnerability Scans

Penetration tests must test the security features of the entity's databases and controls, both from external and internal access.[lii] The proper scope for penetration tests should be evaluated based on the risks identified during the most recent Risk Assessment.[liii]

Vulnerability assessments must be conducted every other year and should involve systematic scans or reviews of information systems. The assessments must be reasonably designed to search for publicly known vulnerabilities identified during the most recent Risk Assessment.[liv]

Application Security

Throughout Part 500, the Department establishes requirements that exceed minimum cybersecurity standards. In order to comply with Part 500, organizations must establish written procedures to ensure security of all applications used within the enterprise, including both software developed in-house and purchased externally.[lv] From an information security perspective, application security is a crucial part of a holistic cybersecurity program. However, application security professionals represent a sub-category in the security discipline. Organizations may want to consider engaging a security professional who specializes in application security in particular in order to comply with Part 500 and – equally importantly – reduce the risk that insecure software could lead to malicious attacks on the entity's information systems and NPI.

Cybersecurity Personnel

Chief Information Security Officer

Entities must have a Chief Information Security Officer (CISO) who bears responsibility for overseeing and implementing the Cybersecurity Program and enforcing policies and procedures.[lvi] In order to have enforcement authority, the CISO must have appropriate backing from key executives, sufficient budget to accomplish their goals, and the authority to exact penalties for noncompliance if necessary.

CISOs can be outsourced to a Third Party Service Provider provided that the entity retains overall responsibility for compliance, designates an employee to oversee the third party CISO and requires the Third Party Service Party to maintain a cybersecurity program that comports with Part 500.[lvii]

The CISO has a few discrete responsibilities for approving any exceptions to two of the NYDFS' most specific requirements. The CISO must approve exceptions to the requirement that remote access to the entity's systems require multi-factor authentication, and exceptions or alternatives to the requirement that NPI be encrypted at rest and in transit.[lviii]

The CISO must annually report to the Board of Directors on the Cybersecurity Program and *material* cybersecurity risks that have been identified.[lix] Part 500 does not define material, so entities are free to determine how they will interpret the term in the context of cybersecurity risks. If applicable, the CISO must consider: confidentiality of NPI, integrity and security of information systems, policies and procedures, material cybersecurity risks, the overall effectiveness of the cybersecurity program and material cybersecurity events.[lx]

The CISO must also annually determine whether the current application security procedures require updating.[lxi]

Additional Cybersecurity Personnel

An entity must employ (in-house) or retain (outsource) personnel with sufficient training to manage the entity's cybersecurity risks and perform the core functions of the Cybersecurity Program.[lxii] Cybersecurity personnel must be trained with cybersecurity updates and the training must be sufficient to address relevant current cyber risks and understand current threats and countermeasures.[lxiii]

Employee Training

Employees must receive awareness training, the content of which must be updated to reflect any issues identified in the most recent Risk Assessment.[lxiv]

Third Party Service Provider Security Policy

Entities must establish written policies for maintaining security against any non-affiliate Third Party Service Provider that has access to NPI or that is permitted to access NPI.[lxv] The policies, which must be based on the Risk Assessment, must also address information systems and NPI that are held by Third Party Service Providers.[lxvi] The policy should stipulate minimum security practices for the service provider, a due diligence process for evaluating adequacy of the service provider's security practices, and take into account whether existing risks are appropriately mitigated by the continued adequacy of the service provider's security practices.[lxvii]

Part 500 goes on to include specific components of a sufficient due diligence process for selecting service providers as well as important contractual provisions. Due diligence should always take into account:

- The service provider's access controls and whether it limits users' access to information systems and NPI[lxviii]
- Whether the service provider requires multi-factor authentication for remote access to information systems and NPI[lxix]
- Whether the service provider encrypts NPI at rest and in transit[lxx]
- Third Party Service Provider contracts should always include the following:
- Provision requiring the service provider to (timely) report cybersecurity events directly impacting an entity's information systems or NPI held by the service provider[lxxi]
- Representations and warranties (as to the service provider's security program and compliance with agreed upon cybersecurity-related obligations). [lxxii]

Incident Response Plan

Each entity must have a written incident response plan (IR Plan) designed to enable quick response and recovery from material cybersecurity events, including those that could halt the continuing function of any aspect of business operations.[lxxiii] Organizations should involve an interdisciplinary team to create an incident response plan which might include , in addition to cybersecurity personnel, human resources, physical security, the legal department, communications, and business section representatives. The IR Plan should:

- Describe goals[lxxiv]
- Define clear roles and responsibilities[lxxv]
- Establish levels of decision-making authority. [lxxvi] (This is useful in the throes of an incident because each role in an incident response team will need to know which other roles may and may not make decisions about each step in the process, e.g., when to notify customers, when to engage outside forensic vendors, and when to remove devices from employees.)
- Establish protocols for external and internal communications and information sharing,[lxxvii] including communication with affected customers[lxxviii]
- Identify necessary remediations or improvements to eliminate information system deficiencies[lxxix]
- Define a process and standards for reporting and documenting events and response activities[lxxx]
- Specify a procedure for evaluating and revising the IR Plan following lessons learned during response activities.[lxxxi]

Information Required to be Provided to Superintendent

Annual Compliance Certification by Board of Directors

In addition to reviewing the CISO's annual report, the Board of Directors must certify to the Superintendent that the entity is in compliance with Part 500.[lxxxii] Each year by February 15, the Board of Directors must affirm by resolution that it has reviewed information sufficiently to determine that the entity is in compliance with Part 500.[lxxxiii] The certification is simple, requiring completion of a short form that affirms compliance[lxxxiv] and should be filed out via the NYDFS' online portal.[lxxxv] No details are required to demonstrate compliance, however documentation to support the Board resolution must be retained for five years and be available for examination by the NYDFS.[lxxxvi]

Cybersecurity Event Reporting – Successful and Unsuccessful Attacks

Within 72 hours of discovering that a Cybersecurity Event has had a reasonable likelihood of harming a material part of the entity's normal operations, the entity must report the event to the Superintendent[lxxxvii]. The NYDFS' FAQs explicitly states that this requirement is meant to include unsuccessful attacks. [lxxxviii] Most unsuccessful attacks would not be reportable under the rule; on the other hand, entities are requested to report particularly significant unsuccessful attacks, such as those that (a) are sufficiently serious to raise a concern at the senior levels of an organization, (b) are not routine in nature, and (c) the organization's resultant precautionary steps are deemed to be extraordinary.[lxxxix]

Events Reportable to Other Regulatory Agencies

If an entity suffers a security incident that is not reportable to the Superintendent (because it is a non-material event according to Part 500) but the incident triggers a reporting obligation to any other authority, the organization must also report the event to the Superintendent[xc]. This does not expand to events that trigger organizations' reporting obligations for disclosures of personally-identifiable information (the subject of most state data breach notification statutes)[xci], but it does double the notice obligation.

Documents in Response to Superintendent Request

The Superintendent may request documents about an organization's Cybersecurity Program and the organization must comply with the request.[xcii] The specific language in Part 500 does not grant the Superintendent the authority to request organization's Risk Assessments, although the Risk Assessment is arguably part and parcel to the Cybersecurity Program.

Documents Required to be Retained

Annual Certification Supporting Documents

The entity must retain documentation to support its annual certification for a period of five years.[xciii] In Part 500, the NYDFS does not elaborate on the extent of documentation required to support the annual certification, so organizations should plan in advance what information to retain and how and when to dispose of information not being retainedThis documentation could be requested in discovery in enforcement actions or civil litigation.

Description of Material Cybersecurity Deficiencies Discovered

If an organization identifies any areas, systems or processes that required material improvement, update or redesign, it must document how the issue was identified as well as the remedial efforts planned and underway to address the issue.[xciv] Such documentation must be available for inspection by the Superintendent.

Audit Logs

The entity must create and maintain an audit system that produces logs sufficient to recreate material financial transactions to support normal operations. Material financial transaction logs must be maintained for a period of five years.[xcv]

The entity must maintain audit logs sufficient to detect and respond to cybersecurity events that a reasonably likely to cause material harm to the entity. Cybersecurity event logs must be maintained for a period of three years.[xcvi] Organizations should examine existing logging functions and enable robust logging where it is not currently enabled.

Enforcement[xcvii]

The enforcement mechanism under Part 500 is unclear; according to subsection 20 of Part 500, the regulation will be enforced pursuant to the "Superintendent's authority under any applicable laws"[xcviii]. Organizations will have to wait and see what actions (or inactions) taken by other entities will trigger an enforcement action. Separately, although Part 500 does not mandate or recommend cyber insurance, organizations may consider checking whether their current cyber insurance policies would cover costs of enforcement actions by NYDFS.

At a Glance: Compliance Deadlines for Part 500 Subsections

Compliance Deadline	Requirement	Reference
August 28, 2017*	Cybersecurity Program; Policies and procedures; Incident Response Plan	500.22(a)
February 15, 2018**	First annual compliance certification submitted via portal	500.17(b); 500.21
March 1, 2018	CISO report to Board on cybersecurity program and material risks	500.04(b)
	Penetration testing and vulnerability assessment	500.05
	Risk Assessment	500.09
	Multi-factor authentication	500.12
	Updated, regular cybersecurity awareness training	500.14(b)
September 3, 2018	Audit trail	500.06
	Application security	500.08
	Secure disposal	500.13
	Monitor authorized users activity to detect anomalies	500.14(a)
	Encrypt NPI in transit and at rest	500.15
March 1, 2019	Third Party Service Provider Security Policy	500.11

- *For any entity seeking exemption from the requirements subject to the August 28, 2017 compliance deadline, it must file its Notice of Exemption no later than September 27, 2017. *See* Section 500.19(e).
- **Certification only applies to subsections currently in force, which for February 2018 includes the adoption of a cybersecurity program and development of policies and procedures. Certification in February 2019 will include the remaining subsections except for the Third Party Service Provider Security Policy subsection, which will be included in the February 2020 certification).[xcix]

At a Glance: Requirements to stay abreast of changing threats and defenses

Required for training cybersecurity personnel	500.10
Required for updating the Risk Assessment	500.09
Required for revising content for employee awareness training	500.14

By grouping requirements such as this one, organizations can create efficiencies in achieving and demonstrating compliance with Part 500.

At a Glance: Activities Required to be Repeated

Repeat Annually
CISO must re-evaluate any exceptions granted to the encryption requirements to determine whether the compensating controls used in place of encryption continue to be sufficiently effective. [500.15(b)].
Penetration test. [500.01(h); 500.05(a)].
Determination of appropriate scope and targets for penetration test based on risks identified in the most recent Risk Assessment. [500.05(a)].
CISO report to Board of Directors. [500.04(b)].
Certify Compliance to Superintendent. [500.17(b)].
Repeat Bi-Annually
Vulnerability assessment. [500.05(b)].
Determination of appropriate scope and targets for vulnerability assessment based on risks identified in the most recent Risk Assessment. [500.05(b)].
Periodically
Risk Assessment. [500.09(a)].
Review access privileges to information systems that provide access to NPI. [500.07].
Review, assess and update Application Security procedures. [500.08(b)].
Assess Third Party Service Providers' security practices to determine continued adequacy. [500.11(a)(4)].
Update Risk Assessment procedures as necessary to address changes to information systems, NPI collected and stored, or business operations. [500.09(a)].
Update training materials for employees to reflect risks identified in the most recent Risk Assessment. [500.14(b)].
Evaluate and revise IR Plan as necessary. [500.16(7)].

At a Glance: Components Expressly Required to be *Written*

Risk Assessment procedure. [500.09].
Policies for protecting Information Systems and NPI on information systems. [500.03].
CISO's annual report to the Board of Directors. [500.04(b)].
Two particular types of audit records. [500.06].
Third Party Service Provider Policy. [500.11].
Incident Response Plan. [500.16(a)].
Documents and reports about cybersecurity events and related activities. [500.16(6)].
Documentation sufficient to support Board of Directors' annual finding that the entity is currently in compliance with Part 500. [500.17(b)].
For any components of the entity's areas, systems or processes that required material improvement, update or redesign, the entity must document how the issue was identified as well as the remedial efforts planned and underway to address the issue. [500.17(b)].

Conclusion

Financial services entities will increasingly find themselves under greater cybersecurity scrutiny by state and federal agencies. Ensuring that proper protocols are in place now will streamline future compliance measures that might be required and, more importantly, help to reduce the risk of cybersecurity incidents or cyberevent.

Even for those entities that have highly developed and mature cybersecurity protections, Part 500 will include additional requirements on regulated entities. As it is an assessment-based model of compliance, cybersecurity policies and procedures need to be tailored to the particular assessments of that entity. While the NYDFS' regulation went into effect in March, the first compliance date was August 28, 2017. By September 27, any entity seeking exemption from the regulation must file a notice of exemption (although even exemptions will still require various aspects of the regulation to be complied with). However, like most other regulations in this area, it will require constant assessment and reassessment, including system testing, risk assessments relating to new software and Board-level engagement and reporting (the first of which will need to be provided by March 1, 2018).

These regulations are now being used as a basis of other pieces of legislation in other states. Given the stricter guidelines around third-party service providers, the regulation follows others in the "weakest link" approach, where the sector is viewed holistically, comprehensively and as critical infrastructure. There is little doubt that the requirements will cascade quickly outside of just New York, given those entities are likely to require the same safeguards from the majority of their vendors, contractors and other stakeholders – whether in New York or elsewhere – and they are likely to require the same, in turn, of theirs.

By Tara Swaminatha and Grace E. King
Tara Swaminatha is a partner and Grace E. King is an associate in the Data Privacy and Cybersecurity Practice of Squire Patton Boggs (US) LLC, http://www.squirepattonboggs.com/

Endnotes

i This article will appear in the September/October 2017 issue of *FinTech Law Report published by Thomson Reuters.*

ii As of the writing of this article, fifteen states have enacted statutes requiring businesses to implement affirmative cybersecurity procedures and practices to safeguard personal information: Arkansas, California, Connecticut, Florida, Illinois, Indiana, Kansas, Maryland, Massachusetts, Minnesota, Nevada, Oregon, Rhode Island, Texas, and Utah. Note, however, that these states vary in what categories of personal data and type of business entities are covered under their respective data security statute.

iii Organizations in other sectors may be subject to their own sector or industry-specific cybersecurity regulations, e.g., the Health Insurance Portability and Accountability Act (HIPAA) sets a standard for cybersecurity compliance in healthcare; while businesses who contract with the U.S. Department of Defense must abide by regulations in the Defense Federal Acquisition Regulation Supplement (DFARS) concerning the provision of specified network security measures to safeguard covered defense information.

iv A "Covered Entity is [any entity] 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." 23 NYCRR Section 500.01(c).

v The following entities are exempt under Section 500.19 Exemptions:

(a) Limited Exemption. Each Covered Entity with: (1) fewer than 10 employees, including any independent contractors, of the Covered Entity or its Affiliates [defined in Section 500.01(a)] located in New York or responsible for business of the Covered Entity, or (2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the Covered Entity and its Affiliates, or (3) less than $10,000,000 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 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(b) An employee, agent, representative or designee of a Covered Entity, who is itself a Covered Entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, representative or designee is covered by the cybersecurity program of the Covered Entity.

(c) 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 shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

(d) A Covered Entity under Article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates) shall be exempt from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16 of this Part.

. . .

(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 that has been accredited or certified pursuant to 11 NYCRR 125.

vi Under Section 500.19(e), a Covered Entity that qualifies for any of the above exemptions pursuant to this section shall file a Notice of Exemption in the form set forth as Appendix B of Part 500 within 30 days of the determination that the Covered Entity is exempt.

vii See supra fn. i.

viii See e.g., New York State Information Security Breach And Notification Act (N.Y. Gen. Bus. Law § 899-AA).

ix Section 500.00 Introduction; 500.17 Notices to Superintendent.

x Section 500.00 Introduction.

xi Section 500.09(b)

xii Section 500.09(b)

xiii Section 500.09(b)

xiv Section 500.09(b)

xxxvii Section 500.02.

xxxviii Section 500.02(b); 500.03.

xxxix Section 500.09(a).

xl Section 500.09(b).

xv Section 500.03.

xvi Section 500.03.

xvii Section 500.04(b); Appendix A of Part 500.

xviii NYDFS Part 500 FAQ #3. Available at http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

xix *See e.g., In re LabMD, Inc., FTC No. 102 3099, Final Order (July 29, 2016); In re ASUSTeK Computer Inc., FTC No. 142 3156, Decision & Order (July 18, 2016).*

xx Section 500.09(b)

xxi NYDFS Part 500 FAQ #10. Available at http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

xxii Section 500.03.

xxiii Section 500.09(a).

xxiv Section 500.09(b).

xxv Section 500.09(a).

xxvi Section 500.09(a).

xxvii Section 500.10(a)(3).

xxviii NYDFS Part 500 FAQ #5. Available at http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

xxix Section 500.09(b)(1).

xxx Section 500.02(a).

xxxi Section 500.02.

xxxii Section 500.02(b).

xxxiii Section 500.09(a).

xxxiv NYDFS Part 500 FAQ #10. Available at http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

xxxv Section 500.02(d). However, information so provided is exempt from disclosure under other applicable laws such as Banking Law or the Insurance Law. *See Section 500.18.*

xxxvi Section 500.02(b)(1).

xli Section 500.02(b)(2).

xlii Section 500.02(b)(3).

xliii Section 500.01(d).

xliv Section 500.02(b)(4).

xlv Section 500.02(b)(5).

xlvi Section 500.02(b)(6).

xlvii NYDFS Part 500 FAQ #9. Available at http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

xlviii Section 500.15(a).

xlix Section 500.15(a)(1)-(2).

l Section 500.15(b).

li Section 500.14.

lii Section 500.01(h).

liii Section 500.05(a).

liv Section 500.05(b).

lv Section 500.08.

lvi Section 500.04(a).

lvii Section 500.04(a)(1)-(3).

lviii Section 500.15(a).

lix Section 500.04(b).

lx Section 500.04(b)(1)-(5).

lxi Section 500.08(b).

lxii Section 500.10(a)(1).

lxiii Section 500.10(a)(2).

lxiv Section 500.14(b).

lxv Section 500.01(n); 500.11(a).

lxvi Section 500.11(a).

lxvii Section 500.11(a)(1)-(4).

lxviii Section 500.11(b)(1).

lxix Section 500.11(b)(1).

lxx Section 500.11(b)(2).

lxxi Section 500.11(b)(3).

lxxii Section 500.11(b)(4).

lxxiii Section 500.16.

lxxiv Section 500.16(b)(2).

lxxv Section 500.16(b)(3).

lxxvi Section 500.16(b)(3).

lxxvii Section 500.16(b)(4).

lxxviii NYDFS Part 500 FAQ #10. Available at http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

lxxix Section 500.16(b)(5).

lxxx Section 500.16(b)(6).

lxxxi Section 500.16(b)(7).

lxxxii Section 500.17(b).

lxxxiii Section 500.17.

lxxxiv Appendix A of Part 500.

lxxxv NYDFS Part 500 FAQ #20. Available at http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

lxxxvi Section 500.17(b).

lxxxvii Section 500.17(a)(2).

lxxxviii NYDFS Part 500 FAQ #5. Available at http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

lxxxix NYDFS Part 500 FAQ #5. Available at http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

xc Section 500.17(a)(1).

xci *See e.g.,* New York State Information Security Breach And Notification Act (N.Y. Gen. Bus. Law § 899-AA).

xcii Section 500.02(d).

xciii Section 500.17(b).

xciv Section 500.17(b).

xcv Section 500.06 (a)(1), (b).

xcvi Section 500.06(a)(2), (b).

xcvii Section 500.20.

xcviii Section 500.20.

xcix NYDFS Part 500 FAQ #16. Available at http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.