January 9, 2023

Submitted via email: cyberamendment@dfs.ny.gov

New York Department of Financial Services
C/O Cybersecurity Division, Attn: Joanne Berman
One State Street, Floor 19
New York, NY 10004

Re: Cybersecurity Requirements for Financial Services Companies (Nov. 9, 2022)

Dear Sir or Madam,

The Securities Industry and Financial Markets Association ("SIFMA")[1] and the Bank Policy Institute ("BPI")[2] (together, "the Associations") appreciate the opportunity to comment on the New York Department of Financial Services' ("NYDFS" or the "Department") proposed second amendment to 23 NYCRR 500 ("Proposed Amendments"). The Associations are deeply committed to the NYDFS' objectives to enhance governance around cybersecurity that the Proposed Amendments are intended to advance. Like NYDFS, our members recognize the critical role cybersecurity plays in building public confidence in financial institutions.

The Associations acknowledge the 2017 effort of the Department to be the first state agency to issue cybersecurity rules for financial services companies and the Department's activities to strengthen the financial services sectors for the benefit of New York State residents. In general, the Proposed Amendments represent an improvement

[1] The Securities Industry and Financial Markets Association ("SIFMA") is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association ("GFMA"). For more information, visit http://www.sifma.org.

[2] BPI is a nonpartisan group representing the nation's leading banks. BPI members include universal banks, regional banks, and the major foreign banks doing business in the United States. Collectively, BPI members hold $10.7 trillion in deposits in the United States; make 68% of all loans, including trillions of dollars in funding for small businesses and household mortgages, credit cards, and auto loans; employ nearly two million Americans and serve as a principal engine for the nation's financial innovation and economic growth. Business, Innovation, Technology and Security ("BITS"), BPI's technology policy division, provides an executive-level forum to discuss and promote current and emerging technology, foster innovation, reduce fraud, and improve cybersecurity and risk management practices for the financial sector.

over the pre-proposal by changing the Class A definition, reducing some of the prescriptiveness, and lengthening the timeframe for compliance. Notwithstanding this progress, we believe that certain elements of the Proposed Amendments can be enhanced to further align with the Department's goals to create a risk-based regulatory framework to ensure and improve the safety and resiliency of the New York financial services industry's digital infrastructure. We respectfully offer the following recommendations for further revision with these objectives in mind.

Executive Summary

The recommendations and considerations discussed at greater length below focus on the following areas:

- **Regulation Scope**: The Associations are very concerned that the Proposed Amendments have significantly expanded the scope of regulated domains, appearing to go far beyond what is customarily considered part of the cybersecurity function and the remit of a Chief Information Security Officer ("CISO") or equivalent. For example, the addition of prescriptive requirements related to business continuity and disaster recovery ("BCDR"), data retention programs, and asset inventory, without explicitly limiting them to cybersecurity-related issues, appears to deviate from the core tenet of what this regulation was set out to achieve. The Associations strongly believe that the Proposed Amendments should be confined to cybersecurity issues, and where adjacent or synergistic domains may be implicated, corresponding obligations should be explicitly tethered to cybersecurity. This approach is consistent with the requirement that the CISO certify a Covered Entity's compliance with the entirety of Part 500.

- **Risk-Based Measures**: The Associations are concerned that in aiming to bolster the risk-based nature of the regulation, the Department has missed its mark, resulting in a rule that has more robust risk assessments but also fewer risk-based controls and an inaccurate presumption of increased risk for Class A companies. As currently drafted, the Proposed Amendments risk adding counterproductive compliance burdens and resource expenditures. As described further below, the Associations urge NYDFS to consider reintroducing risk-based obligations based on the now more robustly defined risk assessments.

- **Materiality Thresholds for Notification Requirements**: The Associations note that the notification requirements to NYDFS have been widened and become more stringent under the Proposed Amendments. At the outset, the Associations urge NYDFS to remove the new notification triggers relating to ransomware events, incidents involving privileged accounts, and events occurring at third party service providers, as incidents in these categories that meet the preexisting materiality threshold would already trigger notification obligations under the current regulation.

Unless these incidents are to be regarded *per se* notifiable, which should not be the case, these additions are redundant. In the alternative, NYDFS could retain and identify these instances as examples of cyber incidents that often, but not necessarily, meet the materiality threshold. This would preserve the ability for Covered Entities to continue making fact-specific analyses and determinations on whether a cybersecurity incident is notifiable. We fully support transparency and realize that regulators seek information on cybersecurity to help the industry as a whole, but we urge NYDFS to achieve these aims together with other regulators through regulatory information sharing, as our membership may often have parallel reporting obligations to other states, federal agencies, and international agencies. This is also an opportunity for NYDFS to harmonize terminology around events, incidents, and reporting with common terminology used by other regulators, including global financial authorities.

- **Governance Proposals for Senior Governing Body**: The Associations wholly support strong governance around cybersecurity. But the proposals around governance would blur the line between the oversight role of the board of directors or senior governing body (the "board") and the day-to-day operational responsibilities of management. The Associations urge NYDFS to refine board-level requirements so that the board can appropriately dedicate its time and efforts to cybersecurity oversight.

- **Independent Audits**: The Proposed Amendments would require Class A companies to conduct an annual independent audit using an external auditor. This is a stark departure from pre-proposal language, which would have allowed the audit to be conducted by independent internal auditors. For the reasons discussed below, the Associations urge NYDFS to permit Class A companies to determine the most effective manner of auditing their cybersecurity programs, including using internal auditors.

- **CISO Requirements and Responsibilities**: The Associations share the Department's goal of supporting the CISO function at Covered Entities. However, the Proposed Amendments add several new requirements and responsibilities for CISOs, which should be reconsidered in light of the way that Covered Entities currently operate. For instance, proposed language relating to a CISO's ability to direct sufficient resources may remove the discretion and authority of a Covered Entity's senior governing body to determine budgeting and resource allocation organization-wide in ways that may have been unintended. Moreover, this language does not reflect the practical reality at our member organizations, where the CISO's decision-making authority regarding budgets, personnel, and other resources for a cybersecurity program is typically not solely within the CISO's discretion but something that often requires cooperation, coordination, and negotiation with other functions within the organization. This level of CISO independence and lack of accountability to

executive management discretion may undermine the financial governance and controls of the overall organization, as well as run contrary to the guidance and mandates of other regulatory agencies. The Associations believe that clarifications on these topics are critical to account for the practical realities of the CISO function within our member organizations.

- **Compliance Certification**: The Proposed Amendments present substantial uncertainty with respect to Covered Entities' ability to certify compliance, especially in light of the expanded definition of what may constitute a violation. Temporary lapses in compliance that are immaterial in nature and subsequently cured should not preclude a Covered Entity from certifying compliance. As described below, NYDFS should clarify that Covered Entities can certify compliance as long as they are fully compliant at the time of the certification and were in material compliance during the prior calendar year. Additionally, the Proposed Amendments require both the CISO and the highest-ranking executive to certify compliance with Part 500. Given the expansive scope of the current regulations, there are significant practical challenges with requiring the CISO to certify compliance with regulatory obligations involving non-cybersecurity-related items. Moreover, the highest-ranking executives at Covered Entities are often a few degrees removed from the implementation of the actual cybersecurity program and therefore are not necessarily appropriate officers to certify compliance. As described below, the Associations urge NYDFS to reconsider its approach to which officers may be responsible for compliance certification.

- **Employers, Agents, Representatives, or Designees of Covered Entities**: The Associations' members rely on the ability for smaller Covered Entities to be covered by the cybersecurity program of an affiliated Covered Entity, including with respect to third party policies, as permitted by Section 500.19(b). As further explained below, the Associations understand that changes to Section 500.11(c) of the Proposed Amendments are not intended to change this framework. To the extent that that is not the case, the Associations would urge that NYDFS reinstate the exemption previously found in Section 500.11(c).

- **Additional Areas of Concern**: The Associations have additional concerns and questions regarding the definition of "qualified party" for purposes of penetration testing, the acceptability of text-based tokens for purposes of multi-factor authentication, and the compliance windows for various provisions.

- **Department Cyber Practices**: The Associations additionally note continued concern about NYDFS' internal data security practices. We understand that NYDFS hired a CISO in the past year, which is a welcome addition. However, given the additional sensitive materials that NYDFS is seeking and will be maintaining on its systems as part of the notification and compliance certification requirements under the Proposed Amendments, the Associations expect that the Department will be reviewing and

enhancing its controls around the safeguarding of sensitive data received from Covered Entities, as appropriate. The safeguarding of and the protection against the unauthorized disclosure of the Covered Entities' sensitive data, particularly information regarding material gaps in compliance, vulnerabilities, and remediation plans, are critical given that this information would significantly increase a Covered Entity's cybersecurity risk profile if exposed, and it could essentially provide a roadmap to attacking a Covered Entity's cybersecurity program if it falls into the wrong hands.

Below are our specific comments and recommendations on areas in the Proposed Amendments that we believe need to be addressed in order to achieve the goal of enhancing governance around cybersecurity and keeping our organizations and ecosystem safe.

Discussion

1. Revive Risk-Based and Outcome-Driven Flexibility in Areas of Prescriptiveness

The Department has been clear that it would like to see Covered Entities conduct more robust risk assessments to support risk-based decision-making. Consistent with this, NYDFS has expanded the definition of "risk assessment" in Part 500.1(n) and the associated requirements in Parts 500.9(c) and (d). With these more robust risk assessment requirements in place, NYDFS need not include more prescriptive measures.

Under the Proposed Amendments, Covered Entities must meet a number of old and new technical requirements that are either (1) not tied to the risk assessment, or else (2) keyed to the now more robustly defined risk assessment, but are nevertheless still subject to very specific prescribed elements. Accordingly, the Proposed Amendments appear to require both a more robust risk assessment AND *de facto* eliminate the risk-based approach that was one of the hallmarks of the original Part 500, thereby limiting the degree of possible tailoring Covered Entities have been afforded to date. Several of the new requirements are granular (for example, asset inventory) and may be impracticable and unable to withstand the test of time. NYDFS should consider replacing these with outcome- or goal-based requirements that allow Covered Entities to achieve those goals with more flexibility.

At the minimum, NYDFS should consider reinstating some degree of risk-based flexibility in several key areas.

Reintroducing a Risk Assessment-Based Benchmark for Certain Technical Requirements: Performing proficient risk assessments across the varying technical components of individual cybersecurity programs takes considerable time. Rather than

prescribing a timeframe, NYDFS should consider ensuring that technical requirement specifications are pegged to the risk assessment across the board. This is currently the case for:

- vulnerability management (including penetration testing (Section 500.5(a)(1)) and vulnerability scanning (Section 500.5(a)(2));
- privileged access management (Section 500.7(a));
- third-party management (Section 500.11)); and
- multi-factor authentication (Section 500.12(a)).

However, this risk assessment-based protocol should be extended to additional requirements such as:

- Class A company controls for privileged access and automated password blocking by adding "Based on a risk assessment" in front of "Class A companies shall also monitor" in Section 500.7(b);
- controls that protect against malicious code, including email and web filtering by adding "as determined by the risk assessment" in Section 500.14(a)(2);
- asset inventory by adding "based on risk assessment" after "shall be maintained" in Section 500.13(a);
- endpoint detection and response, and centralized logging and alerting solutions by adding "as determined by the risk assessment" in Section 500.14(b)(1) and (2);
- encryption by restoring "based on its risk assessment" in Section 500.15(a); and
- multi-factor authentication for all privileged accounts by revising to "privileged accounts based on a risk assessment" in Section 500.12(b)(3).

Allowing for "Effective Alternative Compensating Controls": While it is tempting to require specific controls, Covered Entities with different environments are subject to different risks and often have alternative controls that may be more reasonable and effective. To allow for this, NYDFS should consider consistently providing the option of complying with the technical requirements using "effective alternative compensating controls." Currently, "reasonably equivalent or more secure compensating controls," a higher standard, is provided as an option for a narrow range of requirements, including for automated password blocking (Section 500.7(b)(2)), multi-factor authentication (Section 500.12(b)), and endpoint detection and centralized logging (Section 500.14(b)).

This should be replaced with "effective alternative compensating controls," which are currently only available for encryption at rest (Section 500.15(b)).

The option of "effective alternative compensating controls" should also be extended to requirements for encryption in transit over external networks (Section 500.15(a)) and implementing a privileged access management solution (Section 500.7(b)(1)). This alternative compliance option would allow for a more flexible approach to ensuring data confidentiality and integrity and monitoring and implementing a viable privileged management solution. This will result in compliance that aligns with the technological capabilities of and risks to the Covered Entity, and without undue burden from an operational perspective, such as significantly slower transmission speed due to encryption in transit. For example, our members have relied on data-loss prevention solutions that block sensitive data from being sent outside of their networks as well as dedicated, secure transmission channels to protect data.

Benchmark the Timing of Certain Requirements to the Risk Assessment: As amended, Part 500 currently dictates that many requirements be conducted on a yearly basis. But not all elements need a yearly refresh, and an indiscriminate requirement for an annual assessment cadence for the entire cybersecurity program could draw resources away from areas requiring deeper dives, thus reducing an organization's overall security posture. For example, as amended, Part 500 would require annual audits, annual senior governing body approval of the written cybersecurity policies, annual risk assessments, and annual CISO review of policies, including for application security. Surely, many Covered Entities will conduct these on an annual basis. Yet there may be instances in which other work can and should take precedence.

Understanding this, the Department should encourage Covered Entities to conduct these as-appropriate based on the risk assessment and not at a pre-determined cadence. At the minimum, NYDFS should consider specifically changing the timing requirements for senior governing body approval of policies (Section 500.3), user privilege review (Section 500.7(a)(4)), and application security policies review by the CISO (Section 500.8(b)) to "on a periodic basis, based on risk assessment." This will promote greater focus on the areas needing attention because of known security concerns.

Replace the Class A Distinction with Distinctions Based on the Risk Assessment:

The Class A construct is essentially one in which the NYDFS has determined that a certain "class" of companies have greater risk and require greater controls. But the new risk assessment requirements are designed to identify such risks based on a robust review. NYDFS should consider eliminating the Class A category and make the Class A requirements based on the risk level of data maintained by the Covered Entity, consistent with the newly enhanced risk assessment definition. Such an approach would hew closer to the intent of the Proposed Amendments and promote better cybersecurity.

If NYDFS declines to remove the Class A category, we recommend the Department consider either (a) changing the gross annual revenue threshold to an in-state company's asset threshold, as proposed by IIB in its pre-proposal comment or (b) increasing the definition for Class A status with higher trigger thresholds. As the IIB explained, the asset-based threshold is a better proxy for the size and risk of a bank and is a standard that other regulators use in similar risk-based assessments. Alternatively, NYDFS should consider increasing the revenue threshold to: (1) at least $50,000,000 in gross annual revenue in New York State and over 4,000 employees; or (2) at least $50,000,000 in gross annual revenue in New York State and over $4,000,000,000 in gross annual revenue globally.

Reconsider the Class A Requirement for an Independent Risk Assessment:

NYDFS should consider eliminating the additional requirement for Class A companies to use external experts to conduct a risk assessment every three years. The Proposed Amendments are now much more prescriptive with respect to the parameters of the annual risk assessment Covered Entities are required to undertake. It also requires the assessment to be "reviewed and updated at least annually and whenever [there is] . . . a material change to the Covered Entity's cyber risk." In light of already very onerous obligations, the triennial external risk assessment in Section 500.9(d) would be even more costly, not to mention duplicative of the preexisting general annual risk assessment under Section 500.9(c). Additionally, should NYDFS believe that an external party's review is critical, it should provide the option for that review to be *either* in the independent audit or in the risk assessment, but not both. In the alternative, NYDFS should consider clarifying that the requirement to conduct a risk assessment annually, and for Class A companies to use external experts once every three years, does not necessitate an end-to-end review at each turn or to review each technical component during each assessment. Covered Entities should instead be permitted to comply with the annual risk assessment requirement by ensuring continual updates on appropriate requirements on at least an annual basis and as long as each technical component is assessed at least once every three years.

2. Add Materiality Thresholds in a Number of Places

The final version of the Proposed Amendments should clarify that a materiality standard applies to several provisions in order to avoid significant compliance burdens where there is marginal or limited cybersecurity or resilience benefits for Covered Entities in the absence of such a limiter.

Reporting Obligations: Section 500.4(c) of the Proposed Amendments requires the CISO to "timely report to the senior governing body regarding material cybersecurity issues, such as updates to the Covered Entity's risk assessment or major cybersecurity events." NYDFS should consider adding "material" before "updates" and changing

"major" to "material" before cybersecurity events (and changing "events" to "incidents", *see* Section 4) to ensure that the senior governing body is being updated only about material issues. Elsewhere, we recommend the Department consider using a consistent convention in describing the seriousness of a matter, sticking with "material" instead of "major" and "incident" instead of "event."

Notification Triggers: The Proposed Amendments add three new triggering cybersecurity events requiring notification to NYDFS within 72 hours: (1) unauthorized access to a privileged account; (2) deployment of ransomware within a material part of the Covered Entity's information system; and (3) events at a third-party service provider (Section 500.17(a)(1)(iii), (iv), and (3)).

While the Proposed Amendments incorporate a materiality threshold for the scope of ransomware deployment, they fail to do the same with regard to the actual impact of such an event and for events involving access to a privileged account or third-party service provider. This is inconsistent with the rest of the notification provisions and will impose operational burdens on Covered Entities and result in over-notification to NYDFS with minimal apparent benefit to consumers or the financial industry writ large.

We urge NYDFS to consider, first, whether these additions are truly necessary, given the substantial overlap between them and the existing notification triggers. If an event at a third-party service provider or unauthorized access to a privileged account has the likelihood of materially impacting the Covered Entity or otherwise would result in a notification to another government body, they are already reportable. At the same time, we believe that requiring Covered Entities to report events below the materiality threshold will result in both overreporting and a misallocation of resources both for the reporting Covered Entity and NYDFS.

If removing these additions is not a viable option, then NYDFS should instead consider identifying these events as examples of cyber incidents that often, but not necessarily, meet the materiality threshold. Under this proposal, the entity could determine, based on specific facts, that a ransomware event did not have a material impact on a material part of the Covered Entity's information system and therefore is not notifiable. This option would help keep the materiality threshold risk-based and allow each organization to use its own materiality determination matrix to determine risk. The Covered Entity would be responsible for documenting its decision not to report based on its assessment of the materiality of the event. For example, if a Covered Entity experienced unauthorized access to a privileged account presumptively reportable under Section 500.17(1)(iii), where such event: (1) resulted in access to non-public information; (2) was for a prolonged period of time; (3) was the result of a systemic issue and/or involved multiple privileged accounts; or (4) materially impacted the Covered Entity's systems or data, that Covered Entity would have to report the event. On the other hand, if the Covered Entity did not answer affirmatively to these questions, it would not need to

report. Similarly, a Covered Entity should be required to report that it was affected by a cybersecurity event at a third party service provider only if the Covered Entity: (1) is materially impacted by the third party incident; or (2) is otherwise required to notify another regulator.

Additionally, the Department should consider the practicalities around Covered Entities providing notice of cybersecurity events at third parties. The proposed definition of "cybersecurity event" under Section 500.1(e) captures events that range from interesting, non-impacting occurrences (i.e., unsuccessful events) to full-fledged breaches (i.e., successful events). Applying that definition to the notification trigger regarding events at third parties would be impracticable, since Covered Entities more than likely will not learn of the minor events that occur at their third party service providers. Moreover, requiring Covered Entities to notify immaterial events consumes time and resources that are better directed towards maintaining robust cybersecurity measures.

BCDR Planning: The Proposed Amendments substantially expand a Covered Entity's cybersecurity program from incident response planning to cover BCDR (Section 500.16(a)(2)). While there are substantial overlaps between the disciplines of cybersecurity and wider business resilience, there are also points of difference that should be acknowledged. For instance, ensuring the availability of a business' services goes beyond the technology that supports that service and therefore beyond the competence of the cybersecurity function. Requiring BCDR plans to cover both the wider business continuity elements and the technology and cyber resilience elements could create governance complexity and confusion within Covered Entities. Instead, the requirements under Section 500.16(a)(2) could be expressed as an outcome that the firm must achieve without the prescriptive requirements of where documentation should be located or through which discipline the outcome must be delivered.

Here, too, the Proposed Amendments would benefit from a materiality threshold to avoid diverting resources to non-critical operations, the greater resilience of which is unlikely to result in meaningful benefit to the wider resilience of the entity or the sector. Covered Entities should, and indeed must, have some discretion to determine what business operations are critical in a time of emergency versus those that are only incidental and to prioritize resilience planning for those operations.

Specifically, the BCDR plan in Section 500.16(a)(2) should be designed to "ensure the availability and functionality" of the Covered Entity's *material* services rather than all services, as currently drafted. As currently drafted, Covered Entities would be required to ensure that all services and functionalities, no matter how trivial to the operation of the business, be maintained. This is impractical in practice and counter to the goals of BCDR planning—to enable Covered Entities to maintain necessary operations during emergencies.

Similarly, the requirement to maintain backups in Section 500.16(e) should be clarified to be limited to backups that are material to the provision of the Covered Entity's services and to its operations. Given the costs and environmental impact of maintaining redundancy on servers, requiring Covered Entities to backup *all* of their systems is unnecessarily burdensome, without any apparent corresponding benefit to the Covered Entity. Even though Section 500.16(a)(2)(v) appears to limit the requirement to maintain back-ups to "documents and data *essential* to the operations of the Covered Entity," to avoid any potential ambiguities, Section 500.16(e) should be enhanced to make this limitation explicit; in other words, it should be modified to "[e]ach Covered Entity shall maintain backups *essential to the material operations of the Covered Entity* that are adequately protected from unauthorized alterations or destruction."

Finally, we caution against the mandate that information be stored offsite. While it is one possible method for ensuring availability of backup data in the event of a disruption, offsite storage also has drawbacks, such as creating substantial time delays for restoring that data and expanding potential attack surface. Many firms are exploring alternative methods, such as data immutability. We note that offsite storage is typically understood as different from maintaining backup facilities as per Section 500.16(a)(2)(iv), which is widely considered best practice.

Annual Certification: The Proposed Amendments include a new alternative written acknowledgement provision for Covered Entities that cannot certify compliance to acknowledge they "did not fully comply with all the requirements" of the Part for the prior calendar year. They also clarify that the annual certification must certify that, for the prior calendar year, the Covered Entity complied with the Part. Elsewhere in Section 500.20, the Proposed Amendments state that lapses of 24 hours in compliance are violations of the Part. Read together, it appears that even minor and temporary lapses in compliance, without a realized impact, would prevent Covered Entities from certifying and require a written acknowledgement. As addressed further below, NYDFS should clarify that Covered Entities can certify under Section 500.17(b)(1)(i) as long as they are fully compliant at the time of the certification and were in material compliance during the prior calendar year.

3. Requirements Should Reflect the Senior Governing Body's Oversight Role

Several of the new provisions in the Proposed Amendments appear to reflect an intention for a Covered Entity's senior governing body or board of directors—or their equivalents—to take on a wide-ranging role in the oversight of cybersecurity. While informed and active board oversight promotes sound risk management, in several places, the Proposed Amendments misconstrue the board's fundamental oversight role by dictating how the board must oversee cybersecurity matters and effectively thrusting the board into a position of management rather than oversight. A board should provide

guidance on the organization's strategic direction and plans, monitor management's performance in implementing such plans, and account for the institution's risk appetite, resources, and controls. In this regard, the board should assess and support (and, where deemed appropriate, challenge) management's implementation of the cybersecurity risk management program. Members of the senior governing body, however, should not be expected to serve as cybersecurity risk management practitioners themselves. Therefore, the NYDFS should consider revising the Proposed Amendments to provide boards with the latitude that they need to determine how best to effectively oversee their Covered Entity's cybersecurity program, utilizing their own processes and taking into account the Covered Entity's risk profile and tolerance.

Approval of Cybersecurity Policies: Specifically, Section 500.3 previously permitted each Covered Entity's cybersecurity policy to be approved by a senior officer. The Proposed Amendments would require approval by the senior governing body (e.g., the board or equivalent). Given the specificity and technical nature of the required cybersecurity policies, it is not part of the senior governing body's oversight role to approve them absent taking on a managerial-like function. Further, management should develop, approve, and implement technical—and often voluminous—written cybersecurity policies, standards, and procedures that do not warrant board time and attention. Absent unusual circumstances, the board should be focused on the oversight of enterprise risk management. We believe that it is critical that approval of detailed policies not be permitted to distract the board from its broader functions. The board should maintain candid and informed communication with management about policies to ensure sufficient oversight. In-depth review and approval of cybersecurity policies should be reserved for those hired for their cybersecurity expertise and who have the capacity to manage those policies on a daily basis. To the extent an approval requirement is maintained, it should be more permissive, allowing the senior governing body to rely on summaries or permitting the senior governing body to delegate approval to a senior officer.

Required Expertise: Section 500.4(d)(3) also requires the board to "have sufficient expertise or knowledge, or be advised by persons with sufficient expertise and knowledge." This requirement is overly prescriptive and should instead be framed as the board should "have appropriate understanding of cybersecurity-related matters to facilitate oversight." Boards are, by design, deliberative bodies tasked with oversight of numerous, complex, and inter-related risks, of which cybersecurity is one. To the extent boards, in their discretion, believe they would benefit from additional expertise and insight, they have long found ways to obtain it, including by consulting with independent experts. We believe that a board composed of "special interest" directors is not the best way to advance the collective oversight of these or any other risks, and that Covered Entities are best equipped to identify board members with the collective experience, knowledge, and judgment to oversee the particular risks they face and select and retain competent management. Pressuring Covered Entities to designate directors with

expertise in any single area may adversely impact their ability to identify and appoint directors with other attributes they believe are appropriate for the oversight of enterprise-wide risks their particular institution may face.

Moreover, adding a cyber expert to the board risks diminishing the board's role in oversight, as that one "expert" director may be relied upon by the board as "the" expert. Covered Entities may find that an approach of having a single subject-matter expert results in less effective direction overall, as one individual might organically assume outsized responsibility and authority with respect to a critical risk that is ultimately the responsibility of the collective board to oversee.

NYDFS should refine these requirements so that the senior governing body has sufficient education and knowledge (rather than expertise) to be able to discharge its oversight obligations as a board would discharge any other obligations. At times, this may require external consultation, which should be left to the discretion of the board as a matter of discharging its oversight duties.

Oversight of and Direction to Management: The Proposed Amendments would require the board to "exercise oversight of, and provide direction to management on, the Covered Entity's cybersecurity risk management." The Associations recommend NYDFS strike the language "and provide direction to management on" from Section 500.4(d)(1).

Specific Matters to Be Considered by the Board: In addition to the required report by the CISO to the board addressed above, the Proposed Amendments also require that the senior governing body be advised of "material issues" in the Covered Entity's vulnerability testing (Section 500.5(d)). Material issues in vulnerability testing, which is itself an unclear concept, may not actually be "material" in the more general sense such that they arise to the level of the types of matters that should be reported to the board. Covered Entities are best positioned to determine what information about this topic generally should be reported to the board so as to facilitate effective oversight and should be given that discretion. This is precisely why a CISO is present, and the CISO's management should oversee this, not the board (i.e., in other words, the board should be able to delegate this responsibility to the CISO). If vulnerability testing issues make it to the board, the logical extension is that so should other operational elements across every domain. We recommend that NYDFS refrain from dictating what must be reported to the board and limit the vulnerability testing readout to the executive overseeing cybersecurity. If a prescribed reporting requirement is to be retained, we recommend the Department consider replacing "material issues" with "material vulnerabilities identified" to mirror the intended scope of this section.

4. Notice Requirements

Covered Entities are increasingly subject to a patchwork of reporting obligations that impose different triggers and timelines for notification, often misplacing Covered Entities' focus on meeting notification compliance requirements when an incident occurs rather than focusing on incident remediation. Cybersecurity is a constant battle, both against hackers and for talent, and diverting attention for additional reporting requirements that are already being met elsewhere does not further the mission.

For this reason, our membership has long advocated for harmonization of reporting requirements. Such harmonization can start by working with the Cyber Incident Reporting Council created as part of the recently enacted Cyber Incident Reporting for Critical Infrastructure Act of 2022. NYDFS should consider: (1) harmonizing terminology, definitions, and notification triggers with other requirements; (2) ensuring that reporting is limited to events that have actual material impact on Covered Entities; and (3) revisiting the extortion payment reporting requirements, which do not appear linked to improving or assessing Covered Entities' cybersecurity posture, as we discuss further below.

Harmonize Terminology: The financial industry has persistently advocated for the creation of one common lexicon that includes a definition for cybersecurity "events" and "incidents." There is now a growing consensus among regulators and standard setters globally that cybersecurity events describe occurrences that may or may not create harm, while cybersecurity incidents describe occurrences that create actual harm. In light of this trend, NYDFS should consider including a definition for cybersecurity incidents and utilizing this term when identifying "cybersecurity events that have a material impact," as only successful cyber events (i.e., cybersecurity incidents) have the ability to meet this materiality threshold.

Additionally, while the Proposed Amendments' definition of cybersecurity event is in line with the global financial authorities, the inclusion of a cybersecurity incident definition would serve to strengthen the proposal by removing ambiguity from the test. For example, Section 500.11(b)(3) requires that a Covered Entity be provided notice in the event of a cybersecurity event directly impacting the Covered Entity's information systems or nonpublic information. This could be interpreted to include those events that occur on the third party's system where there was no harm to the Covered Entity's data.

To enable Covered Entities to best map their policies to the cybersecurity requirements of all applicable regulatory regimes and avoid inadvertent compliance gaps due to terminology divergence, NYDFS should consider conforming its terminology to use the term "cybersecurity incident" when describing occurrences that impact the business operations of Covered Entities. Not only would this promote consistency with other regulatory frameworks, but it would also remove ambiguities introduced elsewhere in the Proposed Amendments by the use of the term "cybersecurity event."

Extortion Payments: The Proposed Amendments require Covered Entities to notify NYDFS within 24 hours of an extortion payment being made and within 30 days to provide a more detailed description of the reasons such a payment was necessary. We respectfully submit that such requirements appear punitive rather than constructive or in furtherance of the Part's cybersecurity goals.

Assuming that NYDFS's intention is to gather industry-wide activity patterns or threat trends and not to punish Covered Entities who have determined that ransom payment is necessary, we believe that requiring Covered Entities to provide a detailed description of the reasons underlying their payment decisions is counterproductive and could have a chilling effect on Covered Entities' willingness to otherwise freely share important information with the Department during an incident. Instead, NYDFS could ask for indicators of compromise or other incident-related factual information it can usefully share with industry.

If the NYDFS is concerned that Covered Entities are not engaging in due diligence of threat actors, it could instead require the affirmation of the completion of due diligence and not any underlying reasons for the payment decisions. Our members may consider making extortion payments under extremely limited circumstances: when recovery from backups is not possible, meaning the company is forced to pay to remain operational, or in order to prevent the dissemination of confidential data, including that of our customers. Requiring a further narrative of the rationale for such payments does not appear to serve any valuable goal.

Finally, to counteract the potential hesitancy around sharing the sensitive payment decision, which may already come with complicated reputational implications, we would encourage the Department to consider adopting a safe harbor for reporting under this provision such that Covered Entities who comply with the reporting requirement would not be held legally liable, penalized, or publicly shamed for compliance, and that the reporting would not give rise to an independent investigation of the Covered Entity absent other potential violations of the Part.

5. Permit Independent Audits by Internal Auditors and Clarify the Audit Requirement

The Proposed Amendments define "independent audit" as one conducted by an external auditor and then require Class A companies to conduct an annual independent audit. This is a stark departure from the pre-proposal language, which would have allowed for the audit to be conducted by independent internal auditors. Class A companies should be permitted to determine the most effective manner of auditing their cybersecurity programs, including using internal auditors who meet the independence requirement. This is especially critical if the separate requirement to perform an external risk assessment every three years were to be retained.

First, the internal audit function at most Class A companies is typically robust, competent, and already subject to independence requirements. This is especially true where companies have implemented a three-lines-of-defense model in alignment with federal supervisory requirements. In contrast to external audit firms that are often brought in under an information security budget, internal audit teams are not subject to the direction of the CISO organization. Further, there are often efficiencies when audits are run by internal teams that are already familiar with the cybersecurity function at the Covered Entity and can follow up on previous audits. Many of our members have observed that external auditors may often require more upskill time when it comes to understanding the organization, its systems, procedures, and controls, which has caused undue delay and inaccurate findings in the past. The mandate of an external audit would impose significant additional cost and resource burdens on the Covered Entity with no obvious upside over an internal audit. Finally, should NYDFS choose to keep the "external" requirement, it should clarify whether auditors associated with an affiliate of a Covered Entity could conduct the audit.

Additionally, NYDFS should consider clarifying the scope of the independent audit required for Class A companies under Section 500.2(c) to ensure it focuses on meeting the requirements under the cybersecurity program as opposed to an end-to-end review of the entire program on an annual basis (which can take up to nine months to complete the review and validate findings, and significantly longer to get to a final report stage, and develop plans to address gaps and socialize the results with the appropriate risk governance bodies). As currently written, there is some ambiguity as to whether the required audit should (1) cover compliance with Section 500.2 and any other required elements of a cybersecurity program to the extent not included in one of the Section 500.2(b) enumerated functions, (2) cover compliance with all of Part 500, including, for example, the governance requirements in Section 500.4, or (3) be a different kind of cybersecurity audit, such as a SOC 2 Type 1 or Type 2. Option 1 appears to be the most logical reading of the provision, but further clarifications would be helpful. An annual end-to-end review of the program would become redundant, as most controls do not change month-to-month. Rather, they are updated, matured, and hardened over time.

6. CISO Requirements

The Proposed Amendments add several new requirements and responsibilities for CISOs, which should be reconsidered in light of the way that Covered Entities currently operate.

CISO Resources: The Proposed Amendments require that the CISO be able to "direct sufficient resources to implement and maintain a cybersecurity program" (Section 500.4(a)). This is a modification from the pre-proposal, which required that the CISO have "independence," and is helpful in explaining the contemplated independence. At

the same time, no function in an enterprise has a blank check, and even an "independent" CISO would be subject to scrutiny and review of its proposed budget.

The Associations understand the importance of a CISO's responsibilities and required authority to discharge their responsibilities. However, a Covered Entity's governing body is responsible for taking a holistic view of the Entity and determining resource allocations according to its financial health, business risks (e.g., geopolitical, market, strategic), customer needs, and regulatory obligations. While the CISO is accountable for overseeing and implementing the cyber program, there should be no doubt that the CISO should follow the Covered Entity's budget and resource allocation processes.

As such, a rule that requires the CISO to "direct sufficient resources to implement and maintain a cyber program" runs the risk of pitting the CISO against management. Under such a scenario, Covered Entities could find themselves in violation of this section merely by pushing back on a budget proposal by the CISO. Therefore, the Associations request that the Department remove this language or clarify in another manner that the CISO is not exempt from a Covered Entity's established budgeting and resource allocation process.

Responsibilities beyond Cybersecurity: The Proposed Amendments also introduced certain new requirements that, when read in conjunction with Section 500.4(a), which makes the CISO responsible for overseeing and implementing a Covered Entity's cybersecurity program, appear to impose significant new responsibilities on the CISO, including for areas that currently fall within the mandate of another function. Section 500.3(b)'s newly added "retention" component and Section 500.13's asset inventory requirements are such examples. The Department should consider cabining the CISO's responsibilities to the function's existing mandates and, instead of forcing wholesale restructuring of our members' internal organization schemes, simply require the CISO to coordinate with the functions that are already covering these areas for added accountability and efficiencies.

NYDFS should also consider clarifying the scope of the required BCDR plans, which are intended to be part of the Covered Entity's cybersecurity program. Section 500.16 appears to place responsibility for all BCDR under the CISO. Section 500.16 starts with "[a]s part of its cybersecurity program, each Covered Entity shall establish written plans that contain proactive measures to investigate and mitigate disruptive events and ensure operational resilience, including but not limited to incident response, business continuity and disaster recovery plans." Section 500.16(a)(2) provides that "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 activity." Because the CISO is "responsible for overseeing and implementing the

Covered Entity's cybersecurity program and enforcing its cybersecurity policy" (Section 500.4(a)), one could read these provisions to mean that they place all responsibility for BCDR under the CISO. In practice, however, such responsibility falls under different functions. With all that the CISO must cover, the Associations do not believe that NYDFS intends to expand the CISO's role outside of cybersecurity.

In its final rule, NYDFS should consider explicitly limiting the CISO's responsibilities for BCDR matters to those that are cybersecurity-related and eliminating any ambiguity that might make the CISO responsible for implementing and maintaining BCDR policies beyond cybersecurity. The inclusion of business continuity and disaster recovery within the cybersecurity program of a Covered Entity is an inappropriate expansion of scope and does not align with how many Covered Entities structure such programs and is potentially counterproductive. The broad incorporation of these separate functional areas is also problematic, considering the CISO is expected to certify full compliance but does not oversee all aspects of business continuity and disaster recovery outside of the cybersecurity-related components. Additionally, instead of being responsible for an entity's asset management programs, the CISO should be responsible for aligning the entity's cyber program with its asset management program. In other words, the CISO should not be responsible for all of asset management but should be responsible for incorporating asset management into the cybersecurity program.

7. Reconsider Certifications of Compliance and Acknowledgement Requirements

Compliance Thresholds: NYDFS should consider clarifying the circumstances in which a Covered Entity can certify compliance under Section 500.17 in light of the expanded definition of what may constitute a violation under Section 500.20(b).

Section 500.20 of the Proposed Amendments adds a harsh provision that the "failure to act to satisfy an obligation… shall constitute a violation," and that such failures include the "failure to comply for any 24-hour period" with the regulations. In other words, it appears that *any* time a Covered Entity is not in compliance with the Part for 24 hours, it is a violation of the Part. This would include unfortunate, but commonplace, temporary lapses in implementation that don't result in harm of any kind. For example, a Covered Entity may discover that certain employees' MFA was temporarily misconfigured after the implementation of a patch and there was no evidence of unauthorized use of the account, or the Covered Entity may identify a server that was briefly excluded from vulnerability scanning following a system change. To make clear that only "material" failures to comply constitute violations under the Section, we would recommend striking Section 500.20(b)(2), and short of that, adding "materiality" qualifiers to this section.

While the Proposed Amendments at Section 500.20(c) enumerate a non-exhaustive set of discretionary factors that may be taken into account by NYDFS in assessing penalties for a violation, a temporary lapse in compliance could still be considered a violation, thereby subjecting the Covered Entity to penalties even if one of the discretionary factors were in the Covered Entity's favor, such as the violation being "an isolated incident" or only occurring for a brief period of time. Notably, when read in combination with Section 500.17(b)(1)(i) and (ii), which changes the language regarding a certification, a temporary lapse during the prior calendar year could also prevent a Covered Entity from certifying compliance with the Part.

Moreover, the Proposed Amendments at Section 500.17(b)(1)(i)-(ii) could be read to require a Covered Entity to track and include in an acknowledgement all minor lapses in compliance in the preceding year, even where they have been completely remediated long before the certificate of compliance is due. NYDFS should clarify that: (a) Covered Entities can certify under Section 500.17(b)(1)(i) as long as they are fully compliant at the time of the certification and were in material compliance during the prior calendar year; and that (b) the acknowledgement under Section 500.17(b)(1)(ii) in lieu of a certification is only needed to the extent there are gaps in the Covered Entity's compliance with the Part at the time of the certification.

Compliance Certification: The Proposed Amendments require a Covered Entity's CISO to certify compliance with Part 500 requirements. As explained above, the Proposed Amendments introduce governance and management issues that go beyond the scope of cybersecurity. It would be impractical to require a CISO to certify compliance with regulatory obligations involving non-cybersecurity-related items, such as BCDR issues, data retention program, and asset inventory, some or all of which are within the mandate of other functions (i.e., Risk, eDiscovery, or Technology) at a number of our member organizations. To the extent that the Proposed Amendments go beyond the scope of cybersecurity regulations, the Associations strongly recommend that NYDFS limit these provisions to be co-terminus with cybersecurity issues only, in order for CISO certification to make sense for our organizations. If NYDFS retains its non-cybersecurity-related provisions, it should provide organizations with the flexibility to best determine how to certify compliance. In this regard, the Department should consider replacing the annual certification requirement by the highest-ranking executive and the CISO with certification by the highest-ranking executive *or* a senior officer with the requisite authority to certify compliance from multiple regulated areas (both within and outside of cybersecurity).

The Proposed Amendments also require certification by a Covered Entity's highest-ranking executive. In practice, the highest-ranking executives at Covered Entities are often a few degrees removed from the implementation of the actual cybersecurity program and therefore are not necessarily appropriate officers to certify compliance. If NYDFS is willing to explicitly limit the scope of Part 500 to cybersecurity, then our

members would be comfortable with certification by the highest-ranking executive *or* the senior officer responsible for the cybersecurity program who directly reports to the highest-ranking executive, and the CISO, if different from the senior officer responsible for the cybersecurity program. This would allow for the option for the CISO to serve as the sole certifying officer for a Covered Entity if the CISO directly reports to the highest-ranking executive. If the Department retains the highest-ranking executive certification requirement as currently provided in the Proposed Amendments, our members believe that certification will become a paper-pushing exercise, with CISO certification feeding into the highest-ranking executive's certification with no obvious added benefit from the latter.

If NYDFS is unwilling to adopt our proposal, it should consider extending the compliance window for this provision so that the effective date is greater than 30 days and the provision goes into effect for the 2024 attestation of compliance to avoid any potential delay with the 2023 attestation.

8. Reinstate the Third-Party Service Provider Exemption

The Associations believe NYDFS removed the limited exception in Section 500.11(c) as a cleanup change because the exception, applicable to the broader cybersecurity program, already exists in Section 500.19(b) and remains unchanged in the Proposed Amendments. The Associations welcome this and request that NYDFS clarify that this is indeed what it meant to do. If this was not the case, then the Associations suggest that NYDFS consider reinstating the ability for agents, employees, representatives, or designees of a Covered Entity, who are themselves a Covered Entity, to adopt and rely on the enterprise policies relating to third-party vendors in Section 500.11(c).

Removing the preexisting exemption in Section 500.11(c) and requiring the previously exempt entities to design and implement these policies from scratch will impose unnecessary burdens on smaller Covered Entities who already suffer from resource scarcities. This removal, if intended to supersede Section 500.19(b), will significantly affect how certain of our members currently conduct business and manage compliance. For instance, for Covered Entities with a captive agent field force and who control the agents' use of technology, the removal of the exemption would mean a gross departure from the way the current technology-governance synergy is managed. Furthermore, removing the exemption is not likely to result in improved cybersecurity in practice, just a duplication of policies and procedures.

9. Other Areas of Concern

In addition to the above topics, our members would also like to urge NYDFS to consider the following:

i. Clarifying the meaning of "qualified . . . party" for the annual penetration testing requirement: The Proposed Amendments require each Covered Entity to conduct a "penetration testing . . . from both inside and outside the information systems' boundaries by a *qualified* internal or external independent party at least annually." (Section 500.5(a)(1)) (emphasis added). It is not clear what "qualified" is intended to mean in this context, nor is it clear what standards such qualifications will be evaluated against, if any. NYDFS should consider replacing this qualifier with "competent" and/or "experienced." NYDFS should also consider conforming the usage in Sections 500.4, 500.8(b), and 500.10.

ii. Clarifying the acceptability of text-based tokens for purposes of multi-factor authentication: While the Proposed Amendments remove text message from 500.1(h)(2) as a defined possession factor to be used as part of multi-factor authentication, they do not state that their use is no longer permitted. Accordingly, the Associations understand that while text message-based MFA may be disfavored, it remains permitted.

iii. Extending the compliance window for companies that, under the new rule, either: (1) will no longer qualify for the limited exemption; or (2) will newly qualify as a Class A company: The Proposed Amendments at Section 500.19 replaced the 180-day compliance window for "a Covered Entity [that] ceases to qualify for an exemption" with a much shorter 120-day window. Given the complexity of compliance and the original windows afforded to companies to comply with the regulation, we ask that NYDFS consider extending this period to, at minimum, one year. This will also better align with the compliance windows for new requirements.

iv. Extending the compliance window by at least six months for each of the categories: The Proposed Amendments at Section 500.22 currently provide several compliance deadlines for different categories of requirements, ranging from 30 days to two years from the effective date, with the majority falling in the 180-day category. It goes without saying that it is critical to ensure that the assessments and implementation of controls are done correctly, which requires time. Unreasonable time constraints could force Covered Entities to rush through things, which might lead to unknown gaps and result in heightened risk or the failure of controls where they are needed. Certain technical controls will take a significant amount of time to implement given their prescriptive nature in the Proposed Amendments, and the asset inventory requirement in Section 500.13(a) is a tremendous undertaking for many Covered Entities, requiring significant coordination among internal stakeholders and historical look-back. The asset inventory presumes a data classification system that in itself is a significant undertaking that can take over a year to implement. For larger organizations with multiple Covered Entities and centralized compliance management, the current

timelines are not likely to be attainable, especially if the requirements were to be adopted as presented in the Proposed Amendments. NYDFS should consider extending the compliance deadline by at least six months for each of the categories. Below are recommended extensions for consideration:

- **For 500.17**, the effective date should be greater than 30 days and go into effect for the 2024 attestation of compliance to avoid any potential delay with the 2023 attestation.
- **For 500.2(c)**, the effective date should be greater than 180 days and increased to **at least 18 months** to allow for implementation of controls related to third-party engagement (contracts, sourcing) and completion of such a review.
- **For 500.3**, the effective date should be greater than 180 days and increased to **at least one year** to allow time for larger organizations with many more policies to obtain the necessary approvals.
- **For 500.4**, the effective date should be greater than 180 days and increased to **at least one year** to allow for adjustments to be made to the reporting procedures.
- **For 500.5**, the effective date should be greater than 180 days and increased to **at least 18 months** in light of the significant increase in the scope required for penetration testing and the resulting sourcing and contracting needs for any third parties who may need to be involved.
- **For 500.7(a)**, the effective date should be greater than 180 days and increased to **at least 18 months** to ensure implementation of all new requirements, especially for Covered Entities that need to implement across large matrixed organizations.
- **For 500.9(c) and (d)**, the effective date should be greater than 180 days and increased to **at least 18 months** to implement the large-scale changes to risk assessments in the Proposed Amendments.
- **For 500.12(a)**, the effective date should be greater than 180 days and increased to **at least 18 months** to allow for evaluation of solutions that will need to leverage compensating controls and subsequent review and approval from the CISO.
- **For 500.15**, the effective date should be greater than 180 days and increased to **at least 18 months** due to the increase in scope of encryption and broader application of the requirement, among others.
- **For 500.16(a)(2)**, the effective date should be greater than 180 days and increased to **at least two years** to allow time to evaluate impacts of new requirements and potential solutions required to comply with requirements.
- **For 500.7(b)**, **500.12(b)(2)(3), and 500.14(b)(2)**, the effective date should be greater than 18 months and increased to **at least two years** due to broad

application of the requirement across all platforms and the potential challenges with implementing required solutions to third-party applications where applicable.

If you have any questions or would like to discuss these comments further, please reach out to Brian Anderson at brian.anderson@bpi.com or Melissa MacGregor at mmacgregor@sifma.org.

Respectfully submitted,

/s/ Brian R. Anderson
Brian R. Anderson
Senior Vice President, Technology Regulation
Bank Policy Institute

/s/ Melissa MacGregor
Melissa MacGregor
Managing Director & Associate General Counsel
Securities Industry and Financial Markets Association

cc: Erez Liebermann, Partner, Debevoise & Plimpton, LLP
Thomas Wagner, Managing Director, Technology & Operations, SIFMA

Enclosure: SIFMA/BPI Proposed Redline to Proposed Amendments

SIFMA/BPI Proposed Redline to Proposed Amendments
January 9, 2023

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.

[SIFMA and BPI urge the Department to consider removal of the Class A category or providing asset-based thresholds proposed by IIB. Short of that, we urge the Department to consider increasing the thresholds.]

(c) *Class A companies* mean those covered entities with at least $52~~2~~0,000,000 in gross annual revenue in each of the last two fiscal years from business operations of the covered entity and its affiliates in this State and:

(1) over 42~~1~~,000 employees averaged over the last two fiscal years, including those of both the covered entity and all of its affiliates no matter where located; or

(2) over $41~~1~~,000,000,000 in gross annual revenue in each of the last two 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, regardless of whether the covered entity is 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) *Cybersecurity incident* means a cyber event that: (i). jeopordizes the cyber security of an information system or the information the system processes, stores or transmits; or (ii) violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.

(gf) *Independent audit* means an audit conducted by ~~external~~ auditors free to make decisions not influenced by the covered entities being audited or by its owners, managers or employees.

[(e)] (hg) *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)] (ih) *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)] (ji) *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)] (kj) *Penetration testing* means [a test methodology in which assessors attempt] 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)] (lk) *Person* means any individual or [any non-governmental] entity, including but not limited to any [non-governmental] partnership, corporation, branch, agency or association.

(ml) *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)] (nm) *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)] (on) *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)] (~~p~~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].

(~~q~~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)] (~~r~~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) (~~s~~r) *Third party service provider(s)* means a person that:

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

(2) is not a governmental entity;

(3) provides services to the covered entity; and

[(3)] (4) 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, covering the enumerated functions Section 500.2(b) and other elements of a cybersecurity program required under this Part, 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~~on a periodic basis, based on the risk assessment by ~~[~~a senior officer or~~]~~ the covered entity's [board of directors (or an appropriate committee thereof) or equivalent governing body, setting forth the covered entity's policies and procedures] senior governing body for the protection of its information systems and nonpublic information stored on those information systems. Procedures shall be developed, documented and implemented in accordance with the written policy or policies. 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 cybersecurity-related operations:

(a) information security;

(b) data governance, [and] classification and retention;

(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 and monitoring;

(h) [systems and network monitoring] security awareness and training;

(i) systems and application security and 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 notification; and

(o) vulnerability 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~~ competent 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 authority to ensure cybersecurity risks are appropriately managed~~, including the ability to direct sufficient resources to implement and maintain a cybersecurity program~~. 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, including [and material cybersecurity risks. The CISO shall consider] 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~~ incidents involving the covered entity during the time period addressed by the report; and

(6) plans for remediating material inadequacies.

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

(d) If the covered entity has a board of directors or equivalent, the board or an appropriate committee thereof shall:

(1) exercise oversight of~~, and provide direction to management on,~~ the covered entity's cybersecurity risk management;

(2) require the covered entity's executive management or its delegates to develop, implement and maintain the covered entity's cybersecurity program; and

(3) have ~~sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge, to exercise effective~~appropriate understanding of cybersecurity-related matters to facilitate oversight of cybersecurity risk management.

The title of Section 500.5 is amended to read as follows: [Penetration testing and vulnerability assessments] Vulnerability management.

Section 500.5 is amended to read as follows:

[The cybersecurity program for each] Each covered entity shall, [include monitoring and testing, developed] in accordance with [the covered entity's] its risk assessment, develop and implement written policies and procedures for vulnerability management that are designed to assess the effectiveness of [the covered entity's] its 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:] These policies and procedures shall ensure that covered entities:

(a) [annual] conduct, at a minimum:

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

(2) automated scans of information systems, and a manual review of systems not covered by such scans, for the purpose of discovering, analyzing and reporting vulnerabilities at a frequency determined by the risk assessment, and promptly after any ~~major~~ material system changes;

(b) [bi-annual 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.] have a monitoring process in place to ensure they are promptly informed of the emergence of new security vulnerabilities;

(c) timely remediate vulnerabilities, giving priority to vulnerabilities based on the risk they pose to the covered entity; and

(d) document material ~~issues found~~vulnerabilities identified during testing and report them 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, ~~but at a minimum annually~~ based on the covered entity's risk assessment, review all user access privileges and remove or disable accounts and access that are no longer necessary;

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

(6) promptly terminate access following departures.

(b) To the extent passwords are employed as a method of authentication, the covered entity shall implement a written password policy that meets industry standards. Based on the covered entity's risk assessment, Class A companies shall also monitor privileged access activity and shall implement:

(1) a privileged access management solution or effective alternative compensating controls; and

(2) an automated method of blocking commonly used passwords for all accounts. To the extent a covered entity determines that blocking commonly used passwords is infeasible, the covered entity's CISO may instead approve in writing at least annually the infeasibility and the use of effective alternative compensating controls ~~reasonably equivalent or more secure compensating controls~~.

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~~ competent designee) of the covered entity ~~at least annually~~on a periodic basis, based on the covered entity's risk assessment.

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

(c) The risk assessment shall be reviewed and updated at least annually and 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~~ competent 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~~ competent 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~~ incident directly and materially 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] Except where ~~reasonably equivalent or more secure compensating controls~~effective alternative compensating controls have been implemented and approved by the CISO in writing, 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]

(1) remote access to the covered entity's information systems;

(2) remote access to third-party applications, including but not limited to those that are cloud based, from which nonpublic information is accessible; and

(3) All privileged accounts based on the covered entity's risk assessment.

(c) The CISO shall periodically, based on a frequency determined by the covered entity's risk assessment but at a minimum annually, review any approvals with respect to compensating controls.

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

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 an ~~complete, accurate and documented~~ asset inventory is implemented at the covered entity. The asset inventory shall be maintained based on its risk assessment in accordance with written policies and procedures. At a minimum, such policies and procedures shall include:

(1) a method to track 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:

[(a)] (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) implement controls that protect against malicious code, including those that monitor and filter web traffic and electronic mail to block malicious content, as determined by the risk assessment; and

[(b)] (3) provide [regular] periodic, but at a minimum annual, cybersecurity awareness training that includes social engineering exercises 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~~effective alternative compensating controls:

(1) an endpoint detection and response solution to monitor anomalous activity, including but not limited to lateral movement, as determined by the risk assessment; and

(2) a solution that centralizes logging and security event alerting as determined by the risk assessment.

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 or effective alternative compensating controls, 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 in transit or 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. [(b) To the extent that a covered entity is utilizing compensating controls under subdivision (a) of this section, the] 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] and business continuity management.

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 investigate and 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~~ incident 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~~incidents, 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~~incident;

[(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~~ incidents 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 material cybersecurity-related 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: ***[SIFMA and BPI urge the Department to consider removal of the below prescriptive elements. Short of that, we urge the Department to consider the following modifications.]***

(i) identify cyber-security related 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 cybersecurity-related 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 senior governing body and any other persons essential to the recovery of documentation and data and the resumption of cybersecurity-related 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 cybersecurity-related 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 cybersecurity-related operations of the covered entity ~~and storing of the information offsite~~; and

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

(b) Each covered entity shall ensure that current copies of the plans or relevant portions therein are distributed or are otherwise accessible, including during a cybersecurity ~~event~~incident, to all employees necessary to implement such plans.

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

(d) Each covered entity shall periodically, but at a minimum annually, test its:

(1) incident response plan with all staff critical to the response, including senior officers and the highest-ranking executive at the covered entity, 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 essential to the material operations of the covered entity that are adequately protected from unauthorized alterations or destruction.

Section 500.17 is amended to read as follows:

(a) Notice of cybersecurity ~~event~~incident.

(1) 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~~ incident has occurred that is [either] any of the following:

[(1)] (i) cybersecurity ~~events~~ incidents 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)] (ii) cybersecurity ~~events~~ incidents that have a reasonable likelihood of materially harming, disrupting or degrading any material part of the normal operation(s) of the covered entity;

[SIFMA and BPI urge the Department to consider removal of the added triggers. Short of that, we urge the Department to consider the following alternative.]

(2) The following are examples of cybersecurity incidents that often, but not necessarily, meet the materiality threshold described in Section 500.17(a)(1)(ii):

(i~~i~~) a cybersecurity ~~events~~ incident where an unauthorized user has gained access to a privileged account where the access (a) resulted in access to non-public information, (b) was for a prolonged period of time, (c) was a result of a systemic issue, such as involving multiple privileged accounts, or (d) had a material impact to the covered entity's systems or data; ~~or~~

(i~~i~~~~v~~) a cybersecurity ~~events~~ incident that resulted in the deployment of ransomware that had a material impact on ~~within~~ a material part of the covered entity's information system; or~~.~~

(iii) a cybersecurity incident at a third party service provider in which the covered entity is materially impacted.

(3~~2~~) Within 90 days of the notice of the cybersecurity ~~event~~incident, each covered entity shall provide the superintendent electronically in the form set forth on the department's website any information requested regarding the investigation of the cybersecurity ~~event~~incident. Covered entities shall have a continuing obligation to update and supplement the information provided.

~~(3) Each covered entity that is affected by a cybersecurity event at a third party service provider 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 the time the covered entity becomes aware of such cybersecurity event.~~

(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. Covered entities can certify compliance under this Part as long as they are fully compliant at the time of the certification and were in material compliance during the prior calendar year[.]; 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) to the extent there are gaps in the covered entity's compliance with this Part at the time of the certification, 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 sections of this Part that the entity has not fully complied with and describes the nature and extent of such noncompliance;

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

(*d*) provides remediation plans and a timeline for their implementation.

[SIFMA and BPI urge the Department to limit the scope of the proposed amendments to be co-terminus with cybersecurity issues only.

[Option 1: If Part 500 is not limited to cybersecurity, we urge NYDFS to amend section 500.17(c) as follows]

(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 highest-ranking executive or a senior officer with the requisite authority to certify compliance from multiple regulated areas (both within and outside of cybersecurity). ~~and its CISO. If the covered entity does not have a CISO, the certification or acknowledgment shall be signed by the highest-ranking executive and by the senior officer responsible for the cybersecurity program of the covered entity.~~

[Option 2: If Part 500 is limited to cybersecurity, we urge NYDFS to amend section 500.17(c) as follows]

(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 highest-ranking executive or the senior officer responsible for the cybersecurity program who directly reports to the highest-ranking executive, and its CISO, if different from the senior officer responsible for the cybersecurity program. ~~If the covered entity does not have a CISO, the certification or acknowledgment shall be signed by the highest-ranking executive 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, including [. To the extent a covered entity has identified] all remedial efforts undertaken to address any areas, systems [or] and processes that [require] required material improvement, updating or redesign[, the covered entity shall document the identification and the 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~~ incident involving the covered entity, 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 affirmation that ~~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 has been performed to ensure compliance with applicable rules and regulations including those of the Office of Foreign Assets Control.

d) Safe harbor. Covered entities that comply with the reporting requirement described in Section 500.17(c) will not be held legally liable or penalized for their compliance. Reporting an extortion payment will not give rise to an independent investigation of the covered entity's cybersecurity program absent other potential violations of this Part.

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 and [, including any] independent contractors[,] of the covered entity [or] and its affiliates [located in New York or responsible for business of the covered entity];

(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) An individual insurance broker subject to Insurance Law section 2104, who qualifies for the exemption pursuant to subdivision 500.19(c) of this Part and has not for any compensation, commission or other thing of value acted or aided in any manner in soliciting, negotiating or selling any insurance or annuity contract or in placing risks or taking out insurance on behalf of another for at least one year shall be exempt from the requirements of this Part, provided such individuals do not otherwise qualify as a covered entity for purposes of this Part.

[(e)] (f) 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)] (g) 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 placed in inactive status under Insurance Law section 2103; and individual licensees placed in inactive status under Banking Law section 599-i.

[(g)] (h) 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~~one year 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 material 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 material noncompliance with any section of this Part.~~; or~~

(1) ~~the failure to comply for any 24-hour period with any section 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) The second amendment to this Part shall become effective upon publication of the Notice of Adoption in the State Register.

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

(c) Covered entities shall have 180 days from the effective date of the second amendment to this Part to comply with the new requirements set forth in the second amendment to this Part, except as otherwise specified in subdivisions (d) and (e) of this section.

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

(1) 30 days from the effective date of the second amendment to this Part to comply with the new requirements specified in section 500.17 of this Part, except that covered entities shall have to certify compliance with this Part beginning in 2024;

(2) one year from the effective date of the second amendment to this Part to comply with the new requirements specified in sections 500.3, 500.4, 500.16(e), and 500.19(a) of this Part;

(3) 18 months from the effective date of the second amendment to this Part to comply with the new requirements specified in sections 500.2(c), 500.5~~(a)(2)~~, 500.7(a), 500.9(c) and 500.9(d) ~~500.7(b)~~, 500.12(a) ~~500.12(b)~~, 500.14(a)(2) and 500.14(b), 500.15 of this Part; and

(4) two years from the effective date of the second amendment to this Part to comply with the new requirements specified in sections 500.7(b), 500.12(b)(2) and 500.12(b)(3), 500.14(b)(2), 500.13(a), 500.16(a)(2) of this Part.

(e) The new requirements specified in sections 500.19(e)-(h), 500.20, 500.21, 500.22 and 500.24 of this Part shall become effective on the effective date of the second amendment to 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.