Date: January 6, 2023

To: New York State Department of Financial Services c/o Cybersecurity Division
Attn: Joanne Berman
One State Street, Floor 19, New York, NY, 10004.
Email: cyberamendment@dfs.ny.gov

From: Andrew Moyad, CEO, The Shared Assessments LLC
amoyad@sharedassessments.org
+1-505-466-6434

RE: NYS-DFS Proposed 2nd Amendment to 23 NYCRR500 Cybersecurity Requirements for Financial Services Companies

The Shared Assessments Program appreciates the opportunity to submit comments to the New York State Department of Financial Services, Cybersecurity Division.

Shared Assessments has been setting the standard in third party risk assessments since 2005. Shared Assessments, which is the trusted source in third party risk assurance, is a member-driven, industry-standard body which defines best practices, develops tools, and conducts pace setting research. Shared Assessments Program members work together to build and disseminate best practices and develop related resources that give all third party risk management stakeholders a faster, more rigorous, more efficient and less costly means of conducting security, privacy and business resiliency control assessments. Additional information on Shared Assessments is available by visiting: http://www.sharedassessments.org.

On behalf of the Shared Assessments Program and its members, thank you for accepting the following response in regard to the proposed NYS-DFS Proposed 2nd Amendment to 23 NYCRR500 Cybersecurity Requirements for Financial Services Companies.

Shared Assessments Proposed Regulatory Amendment Response Re: *NYS-DFS Proposed 2nd Amendment to 23 NYCRR500 Cybersecurity Requirements for Financial Services Companies*

Thank you for the opportunity to provide a response to the ***NYS-DFS Proposed 2nd Amendment to 23 NYCRR500 Cybersecurity Requirements for Financial Services Companies*.** Our responses below address our specific comments by section of the Amendment.

Proposed Amendment to 500.1 Definitions:

Response: The definitions as written provide key clarifications for content added in the proposed Amendment. The risk-based approach that resonates throughout the Amendment is commendable and provides robust and appropriate practice guidance.

NYS DFS should consider different metrics to better define a "Class A company." Too many trading platforms and money movement services are thinly staffed yet manage a considerable amount of economic risk. In fact, the proposed revenue or employee count approach does not meaningfully correlate with risk exposure. We believe an alternative approach better tied the measurement of material risk, such as economic throughput (e.g., dollars wired, or securities traded) or volume of client records, is a more meaningful risk metric to define this class of business.

Rationale: Where Nth party considerations arise, emphasis should be made that the supply chain parties that require special attention before onboarding and ongoing due diligence are only those third (and Nth) parties which are critical providers (as determined by the outsourcer in their risk assessment processes). Other ESG regulations may require a more expansive Nth party review depending on the overarching law. With reference to section (c) definition of "Class A companies," the annual revenue cap is from the covered and all affiliates in the State. With reference to section 500.1 (c) definition of "Class A companies," where the annual revenue cap is from the covered and all affiliates in the State. Is it feasible and appropriate to classify based on ALL revenue, or should this be only that revenue that is in scope with in NYS, or where there are common processes across those business lines that might pose vulnerabilities? For firms where OCC minimum standards are already being met, this would not be an issue. This applies to all industry, making the logic plausible, but needs to be explicitly stated. For firms where OCC minimum standards are already being met, this would not be an issue.

Proposed Amendment to 500.2 Cybersecurity Program:

Response: We agree with this change as drafted as this requirement is risk-based and provides for each entity's unique environment and needs, allowing for due diligence and response planning appropriate to the evolving landscape. We recommend that the periodicity of an independent audit for Class A companies of the internal to the regulated organization's cybersecurity program cycle should be changed from "at a minimum annually" to mirror the requirement in Section 500.9 to read: "…and whenever a change in the business or technology causes a material change to the covered entity's cyber risk."

Rationale: While this section does not specify the requirement for third party inventory, this can be intuited from the language in the amendment and is included specifically through this proposed Amendment in Section 500.13. There is an existing expectation that the assessment of the entity should ensure the requirements of any party has the same as those the third party is being held to and are being performed upon it. This strengthens the whole supply chain and supports the reasoning behind the Amendment. While the Nth party may not be regulated in the same manner as the regulated entity, the onus still falls on the outsourcer to manage and provide to the regulators "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."

Proposed Amendment to 500.3 Cybersecurity Policy:

Response: As written, this revised language is good and complete. The revision to (c) improves the existing rule with "asset inventory, [and] device management and end of life management;" however, IoT (Internet of Things) should have a special carve out in asset management (section 500.13), with focus placed on that set of devices and network connections with the intention of changing how IoT is managed within the industry as a whole. Software Bill of Material (SBOM) is sufficiently important that it should be called out in section (i) of 500.3 "… systems and application security and development and quality assurance; …" The SBOM was recently included in a Biden Administration Executive Order and must be maintained by vendors who sell software to the federal government. Robust language would include device management for any equipment that touches a network, including mobile device management (MDM). Connecting any IoT device to the organization or agency network should require prior approval from a designated information security office.

Rationale: Asset inventory is undervalued—this includes IoT devices. Another asset management area that remains problematic, especially in the insurance industry, is agents and brokers/managing agents that have access to protected information; yet do not/may not have the same security requirements. The Amendment does not directly address how that population of "non-traditional" third parties be handled; however, those non-traditional parties pose the same risk that traditional parties pose. Approval for IoT devices is a human-driven process. Best practice for that process includes the use of AI monitoring of device behaviors and auto-quarantining devices, as required (2021 Shared Assessments/Ponemon Institute IoT Report).

Proposed Amendment to 500.4 [Chief information security officer] Cybersecurity governance:

Response: We agree that mandating independent freedom of action (i.e., stature) to assemble the resources is essential and necessary to carry out cybersecurity governance. We have three recommendations regarding this section. (1) CISO conflict of interest language should be added to ensure CISOs are not recruited from the organization providing significant services to the (likely very small) institution. While the points carved out in (a) through (o) are complete, there is an inherent conflict of interest in the two-hat loyalty created if CISO is not independent. (2) The Amendment needs to provide clarification around what is meant by the term 'sufficient' – "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." We recommend that the language could be revised to note that: "At least annually, the CISO should review with the Board of Directors (or equivalent) the organization's cyber security resource adequacy, disclosing any deficiency that impedes the efficiency or effectiveness of the program." (3) While the requirement is set for CISO to report to a governing body, there is not a requirement for the body to take action to correct any assessed issues. This needs to be referenced directly, even though it is noted in another context in Section 500.5, where the language around Vulnerability Management reads: (c) "timely remediate vulnerabilities, giving priority to vulnerabilities based on the risk they pose to the covered entity…"

Rationale: The CISO reporting directly to the board is not common practice, as evidenced by the Ponemon Institute survey that demonstrates less than half of cybersecurity leaders say they report directly to the board. Among those that do, the frequency of their briefings is 13% annually, 15% bi-annually, 30% quarterly, and 51% only when a security incident occurs (How CISOs Can Wield More Power in Organizations, December 5, 2022, Wall Street Journal). (1) A CISO cannot be sourced from an existing provider that would be assessed and monitored. This would be of particular note in smaller firms where the entity (the bank) may have to manage multiple levers to retain providers they need to be able to stay in business and still improve their cyber posture under scrutiny of an independent CISO. (2) The standard to meet is: "appropriately managed." While the CISO is provided with stature to report, there should be some requirement on the governing oversight that the governing body will take action in the form of a reasonable and timely response. Where the term 'sufficient' is used, what is the expectation regarding the covered entity's documentation as part of the reporting requirement that would demonstrate that the entity has met the requirement for 'sufficiency?' (3) The letter of the amended Rule does not require a

response from the governing body once the CISO makes a Report on a gap or other issue. This should be addressed before the Amendment is finalized.

Proposed Amendment to 500.5 [Penetration testing and vulnerability assessments] Vulnerability management:

Response: The language represents good, robust practice that is risk-based.

Rationale: This section accurately covers assessment, monitoring (including continuous monitoring), and remediation of vulnerabilities as part of due diligence to determine that the service provider engaged is able to perform the necessary tasks on the outsourcer's behalf (including protection of systems/data) in the event of disruption.

Proposed Amendment to 500.7 Access privileges and management:

Response: The use of the terminology throughout the draft is 'based on the covered entity's risk assessment,' which perfectly reflects the practical aspects of risk management at its best. The limits listed in this section may not be adequate for the stated intention of the Amendment. For example, cloud environments may pose vulnerabilities which are not addressed. In addition, the criteria used to determine access privilege and management must take into account the fluidity of an organization's employee base and how that can change relative to roles and responsibilities across areas of business. The stated limit to an annual minimum is not adequate, this should instead be "regularly, at intervals that take into account shifting employees roles and responsibilities." Unannounced checkpoints (training, clarity, surprise yields insight) may otherwise be clouded/shadowed.

Rationale: This seems consistent with the well-established practice that access to systems should only be allowed to those who require such access to perform their job functions. However, the language noted in subsection (3) "limit the use of privileged accounts to only when performing functions requiring the use of such access;" could better convey the concept of privileged access criteria.

Proposed Amendment to 500.8(b) Procedures, Guidelines & Standards:

Response: We recommend that the language in 500.8(b) be updated to note that annually may be insufficient in some circumstances. A possible revision that would address this is: "All such procedures, guidelines, and standards shall be [periodically] reviewed, assessed, and updated as necessary by the CISO (or a qualified designee) of the covered entity at least annually or at intervals organization specified triggers mandate the need for revisions, such as roles that include privileged access and financial reporting."

Rationale: This recommendation is consistent with, for instance, Section 500.9, which reads: "… and whenever a change in the business or technology causes a material change to the covered entity's cyber risk."

Proposed Amendment to 500.9(c) and (d) Risk Assessment:

Response: We suggest that term "external expert" be defined, as it is currently not defined in Section 500.1 of the Amended Rule, or in the DFS online Glossary. We suggest a definition such as that used in the European Union's EU's Digital Operational Resilience Act (DORA) (para 6, p. 182), which reads: "The independent experts referred to in paragraph 4, second subparagraph, shall be appointed by the Oversight Forum from a pool of experts selected following a public and transparent application process." Establishing a pool of auditors that are independent (and/or may be hired by independent parties). Their language further bounds how expertise is determined: "The independent experts shall be appointed on the basis of their expertise in financial stability, digital operational resilience and ICT security matters. They shall act independently and objectively in the sole interest of the Union as a whole and shall neither seek nor take instructions from Union institutions or bodies, from any government of a Member State or from any other public or private body."

We also recommend that the periodicity of the use of external experts for Class A companies to "conduct a risk assessment at least once every three years" mirror the NYS DFS Amendment requirements for all companies which reads "… at least annually and whenever a change in the business or technology causes a material change to the covered entity's cyber risk."

Rationale: In the existing DFS Rule, external experts are not required for program audits, allowing for internal audit teams to conduct assessments and other reviews as long as they were truly independent. It is our opinion that requiring an independent expert to be external to the outsourcer could be an untenable cost burden for small and medium financial services entities.

Proposed Amendment to 500.10 Personnel & Intelligence:

Response: The proposed language is sufficient to address the risks being considered in this section.

Rationale: The proposed language is adequate.

Proposed Amendment to 500.11 Third party service provider policy:

Response: The requirements for real-time due diligence assessments within the Amendment are not comprehensive. It is consistent with best practices, except for there being no language for policies/procedures to be reviewed at least annually, or "regularly, at intervals that take into account shifting employees roles and responsibilities."

Rationale: The requirements to meet "minimum cybersecurity practices required to be met by third parties…" is not adequate to provide for periodic assessment where appropriate (e.g., continuous monitoring is not specified).

Proposed Amendment to 500.12 Multi-factor authentication:

Response: This content points to another reason for independence in Subsection (b) of this section, due to need for approval by an independent CISO.

Rationale: A CISO cannot be sourced from an existing provider that would be assessed and monitored. This would be of particular note in smaller firms where the entity (the bank) may have to manage multiple levers to retain providers they need to be able to stay in business and still improve their cyber posture under scrutiny of an independent CISO.

Proposed Amendment to 500.13 [Limitations on] Asset management and data retention requirements:

Response: While the Amendment to Section 500.3(c) improves the existing rule with "asset inventory, [and] device management and end of life management," the IoT (Internet of Things) needs to have a special carve out in asset management, with focus placed on that set of devices and network connections with the intention of changing how IoT is managed within the industry as a whole. Section 500.13 could include a requirement for this timely update to IoT asset management that would help build a better understanding, for example of IoT related risks, that has heretofore been difficult for outsourcers to gauge.

Rationale: The Asset management language as written is welcome and overdue. This language would do well to include IoT obligations. Regarding the profound need to add IoT language, four cycles of research with the Ponemon Institute research confirms that the processes around IoT at many firms are grossly inadequate. Shared Assessments/Ponemon Institute IoT research surveys have repeatedly revealed that few to any organizations have an accurate (current) inventory of their IoT devices, and many do not document the majority of those devices.

Proposed Amendment to 500.14 [Training and monitoring] Monitoring and training:

Response: The revisions to this section are adequate as written.

Rationale: There are no shortcomings noted in the proposed language.

Proposed Amendment to 500.15 Controls - Encryption:

Response: This response is reasonable.

Rationale: Alignment with prevailing practice facilitates and simplifies compliance.

Proposed Amendment to 500.16 Incident response [plan] and business continuity management:

Response: Taking into account learning from incidents, as noted in Subsection (vi) "…identify third parties that are necessary to the continued operations of the covered entity's business, …" there is a need to also ensure that the down chain critical (Nth) parties have the same resilience, the same controls, monitoring, etc. Therefore, in testing Subsection (d), the section needs to include "third parties that are necessary for the resilience of the service." This is also true for Subsection (e) where cloud and/or hardened equipment could pose an issue. IR Plans should ensure timely/and non-electronic plan availability for distribution to IR participants. Identification of alternate communication and payment systems.

Rationale: The language in (3) around the ability to restore its systems from backups would be inadequate without (e), which makes it robust.

Proposed Amendment to 500.17 Notice of cybersecurity event:

Response: Cyber event should include any event that includes access to data that includes personally identifiably information (PII), privileged corporate information, or any other type of sensitive information. That reference is necessary in the enumerated events with this Section.

Rationale: It would be useful for the DFS to aim for harmonization of notification across jurisdictions (e.g., US/EU/UK/NA-SA/Asia PAC) to provide some rationalization of notification and notice of extortion payments, such that one fits all (or most) that can be communicated broadly. The rule for reporting within 72 hours after determining a cyber incident has occurred, which is dictated by the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) | CISA, could be mirrored by DFS as an essential standard in the interests of uniformity, unless national or international security was at risk. A 72-hour timeframe also mirrors the European Union's GDPR notification requirement for cybersecurity events. By tying to existing domestic and international requirements, DFS will be aligned with at least two key regulatory frameworks that are considered best practice globally and be less likely to come into conflict with compliance through any departure of the 72-hour timeline. Likewise, any regulatory standard more rigorous than 72 hours would complicate how firms go about notifying multiple stakeholders.

Proposed Amendment to 500.19 (a), (e), (f) and (g) Limited exemption:

Response: With reference to section 500.1 (c) definition of "Class A companies," where the annual revenue cap is from the covered and all affiliates in the State, is it feasible and appropriate to classify based on ALL revenue, or should this be only that revenue that is in scope with in NYS, or where there are common processes across those business lines that might pose vulnerabilities. For firms where OCC minimum standards are already being met, this would not be an issue.

Rationale: This applies to all industry, making the logic plausible, but needs to be explicitly stated. For firms where OCC minimum standards are already being met, this would not be an issue.

Proposed Amendment to 500.20 Enforcement:

Response: This response is reasonable.

Rationale: The language as drafted is inclusive of the needs of the agency around enforcement and is clearly written for companies that are being regulated.

Proposed Amendment to 500.21 Effective date:

Response: When would the annual reporting requirement begin (calendar year)? Nothing should change, given the rule has been in place for five years.

Rationale: The timeframe given for the effective date is reasonable.

Proposed Amendment to 500.22 (c), (d) and (e) Compliance date:

Response: The proposed language is elaborating an existing DFS framework.

Rationale: The timeframes are reasonable.

Proposed Amendment to 500.24 Exemptions from electronic filing and submission requirements:

Response: The proposed language is reasonable as drafted.

Rationale: The requirements are reasonable.