EVERSHEDS SUTHERLAND

THE Committee OF Annuity Insurers
www.annuity-insurers.org

January 9, 2023

VIA E-Mail
Joanne Berman
New York State Department of Financial Services
One State Street
New York, NY 10004

Re: **Comments on Proposed Second Amendment to 23 NYCRR 500**

Dear Ms. Berman:

This comment letter is submitted on behalf of the Committee of Annuity Insurers (the "Committee" or "we").[1] The Committee is pleased to have the opportunity to offer its comments on the New York State Department of Financial Services' (the "Department") Proposed 2nd Amendment to Regulation 23 NYCRR Part 500 (November 9, 2022) (the "Proposal").

Committee members applaud the Department's goals in proposing the amendments to 23 NYCRR Part 500. The comments in this letter reflect the Committee members' consideration, and concerns with certain aspects, of the Proposal, so that the final amendments will enable individual Committee members to effectively and efficiently implement the final amendments.

The Committee is also aware that other insurance and financial services industry groups, including the Life Insurance Counsel of New York ("LICONY"), are submitting comments expressing similar concerns to those expressed in this letter. The Committee is supportive of those comments, and urges the Department to take seriously the significant and real concerns raised by industry regarding the Proposal.

[1] The Committee is a coalition of many of the largest and most prominent issuers of annuity contracts. The Committee's current 30 member companies represent approximately 80% of the annuity business in the United States. The Committee was formed in 1981 to address legislative and regulatory issues relevant to the annuity industry and to participate in the development of insurance, securities, banking, and tax policies regarding annuities. For over three decades, the Committee has played a prominent role in shaping government and regulatory policies with respect to annuities at both the federal and state levels, working with and advocating before the SEC, CFTC, FINRA, IRS, Treasury Department, and Department of Labor, as well as the Department, the NAIC and the relevant Congressional committees. A list of the Committee's member companies is available on the Committee's website at www.annuity-insurers.org/about-the-committee/.

Eversheds Sutherland (US) LLP is part of a global legal practice, operating through various separate and distinct legal entities, under Eversheds Sutherland. For a full description of the structure and a list of offices, please visit www.eversheds-sutherland.com.

1. Proposed Board Requirements and Obligations Would Undermine the Role of the Board and Could Compromise the Effectiveness of Corporate Risk Management and Governance Functions

The Committee is concerned that the Proposal includes provisions that would require boards of directors to undertake a detailed managerial role that would undermine the board's essential independent oversight role. Mandating the board to "provide direction to management" on cybersecurity risk management is fundamentally inconsistent with the appropriate segregation of roles between a board and management, and would actually reduce the effectiveness of corporate risk management and governance by breaking down the checks and balances between the board's and management's distinct roles and responsibilities.

Specifically, **Section 500.4(d)** of the Proposal would require boards (and equivalent bodies) to "exercise oversight of, and provide direction to management on, the covered entity's cybersecurity risk management." The Proposal would also require the board "to have sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge, to exercise effective oversight of cybersecurity risk management."

The requirement to "provide direction to management" in particular undermines the independent oversight role of the board by requiring that board members be directly involved with the ongoing management of the covered entity's cybersecurity program, a role that is appropriately the job of management. By doing so, the Proposal would actually break down the three lines of defense that generally define a mature governance, risk, and compliance regime, thereby reducing the independence of the board from the management of the company and actually decreasing the strength and maturity of the risk oversight and management framework at covered entities. [2] This same concern applies to the new requirements proposed under Section 500.3 (requiring annual approval of the cybersecurity policy by the board), Section 500.4(c) (CISO must timely report to the board on material cybersecurity issues), and Section 500.5(d) (requiring material issues found during penetration testing to be reported to the board).

The Committee agrees that it is important for the board to remain engaged and appropriately informed regarding cybersecurity risk and the risk management activities of a covered entity, but doing so should not mean giving direction to management of the covered entities cybersecurity program. We suggest that the proposed requirements referenced above be revised or reframed to clarify that the board is not expected to participate in the direct management of the covered entity's cybersecurity program. We suggest that these concepts would be better addressed through a separate requirement for covered entities to keep their senior governing body appropriately informed of the covered entity's cybersecurity risks, risk management activities, material cybersecurity issues, and significant updates or changes to its cybersecurity program so that the board can exercise effective oversight.

---

[2] Under the three lines of defense framework developed by The Institute of Internal Auditors ("IIA"), the following high-level roles typically define a mature governance, risk, and control/compliance regime:

- The Governing Body accepts accountability to stakeholders and delegates responsibility to management for achieving objectives.
- Management's responsibility is to achieve organizational objectives (including legal, regulatory, and compliance expectations) comprises both first and second line roles. First line roles are most directly aligned with the delivery of products and/or services to clients of the organization, and include the roles of support functions. Second line roles provide assistance with managing risk and provides analysis and reporting on the adequacy and effectiveness of risk management to the Governing Body.
- Internal audit provides independent and objective assurance and advice on the adequacy and effectiveness of governance and risk management to Management and the Governing Body.

More information on the IIA's Three Lines Model is available at https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf.

2. The Proposal Prescribes a Scope and Role for the CISO That Is Inconsistent with Common Practices

The Proposal appears to require the CISO to be ultimately responsible for a range of functions that, in practice, are often not within the CISO's purview. For example, Part 500 includes provisions addressing customer data privacy (§ 500.3(k)), business continuity and disaster recovery (§ 500.16) ("BCDR"), and audit responsibilities (§ 5003(c)). All of these domains appear to be considered part of the required overall cybersecurity program, which must be overseen and implemented by the CISO (§ 500.4). The CISO is additionally required to sign the certification of compliance with all these requirements under Section 500.17(b)(2) of the Proposal.

However, in practice, CISOs are not generally directly responsible for all of these areas. Consumer privacy is generally run by a Chief Privacy Officer; audit is run by an internal audit function; and BCDR is usually owned by a range of other senior officers. Nonetheless, the Proposal appears to require that all of these rolls be consolidated under and managed at least to some extent by the CISO. Such a requirement would require corporate restructuring in many cases, and runs against industry best practices for managing these important functions.

The Committee requests that the proposal be revised to clarify that the CISO is not required to oversee all functions required under Part 500, but rather that the CISO may satisfy these requirements in coordination with other senior staff members responsible for functions that meet the requirements of Part 500.

Additionally, the CISO should not be required to sign a certification of compliance with respect to areas that are not within the CISO's purview. Rather, the certification should be required to be submitted in the name of the covered entity directly, while being based upon documentation that includes assertions from appropriate officers and employees of the covered entity based on the covered entities business operations, including the CISO.[3]

3. The New Punitive Definition of a "Violation" and Strict Standard for Compliance Certification Are Unworkable

Section 500.20 of the Proposal establishes a new definition for what constitutes a violation of Part 500. This new definition is overly punitive in approach, and creates an overly strict standard for when a covered entity is eligible to file a certification of compliance.

The Proposal would define a violation to include the failure to "prevent unauthorized access to an individual's or entities nonpublic information due to noncompliance with any section of this Part." This suggests that any occurrence of a data breach creates a functional presumption of a possible violation of the Part 500 requirements, particularly in the context of the Section 500.2 requirement to design a cybersecurity program that protects the confidentiality of nonpublic information ("NPI"). We believe that this is an inappropriate and overly punitive standard to set, particularly in light of the fact that data breaches are perpetrated by active and malicious bad actors. An unfortunate reality of cybersecurity today is that data breaches are inevitable. No organization can hope to be completely impenetrable over time. Accordingly, we request that **Section 500.20(b)(1)** be deleted. A violation should be based solely on non-compliance with the requirements of Part 500, not whether a breach has occurred.

Section 500.20(b)(2) defines a violation to include <u>any</u> failure to comply with <u>any</u> section of Part 500 for any 24-hour period. This definition of a violation results in an overly rigid standard for compliance. **Section 500.17(b)** would require a covered entity to file an acknowledgement of non-compliance any time the entity "did not fully comply with all requirements" of Part 500. When paired with the Proposal's new definition of a "violation" of Part 500 that includes non-compliance for any 24-hour period, even minor and non-material gaps in compliance could prevent covered entities from filing a certificate of compliance. This approach is inconsistent with the practical realities of running an enterprise compliance

[3] Similarly, the Proposal would require the highest-ranking executive officer to sign the certification, regardless of whether the officer would otherwise play a significant role in cybersecurity or other issues addressed by Part 500. Requiring the executive to sign the certification would also present significant administrative challenges without providing a substantive benefit to the overall compliance and risk management process. It is also unclear how this requirement would work with portal filing processes. Would the CEO and CISO be required to directly log into the DFS portal to manually submit annual certification?

program, which is designed to identify and remediate compliance shortcomings as part of the normal and expected operations of a covered entity.

The Committee requests **Section 500.20(b)(2)** be deleted, and that the Proposal clarify that non-material compliance issues that are remediated within the normal course of operations do not prevent a covered entity from submitting a certification of compliance under Section 500.17.

4. Annual External Audit Requirement Should Be Further Clarified

Section 500.2(c) of the Proposal would require Class A companies to conduct an "independent audit of their cybersecurity programs at least annually". "Independent audit" would be defined as an audit "conducted by external auditors…."

This external audit requirement is different from the pre-proposed version, which would have appropriately allowed an independent internal audit function to satisfy this requirement. Requiring an external audit annually is an overly burdensome obligation that would require covered entities to expend significant time and resources, while serving only a limited substantive purpose for a cybersecurity program that will not change materially from year to year. Additionally, requiring annual external audits could cause capacity issues in the marketplace, which must support this requirement with qualified and capable external auditors.

The Committee proposes that an independent internal audit should be permitted to meet this requirement or, at a minimum, the frequency of the external audit should be decreased to align with the 3-year external risk assessment requirement.

We also request clarification, whether in the final amendments or through guidance, on the required nature and scope of the audit. Would existing industry audit standards, such as SOC 2 Type II audit, be sufficient to comply with this audit requirement?

5. Overly Rigid Cybersecurity Event Notice Requirements Should Be Modified

The Proposal expands the existing requirements to notify the Department of cybersecurity events by requiring notice of any compromise of a privileged account or event affecting a service provider regardless of materiality. This proposed requirement creates overly strict affirmative notice requirements that should be modified.

Section 500.17(a)(1)(iii) of the Proposal would require covered entities to notify the Department of any cybersecurity incident that involves the compromise of a privileged account, regardless of the nature or materiality of the compromise. Similarly, **Section 500.17(a)(3)** would require covered entities to notify the Department of <u>any</u> cybersecurity event at a third party service provider of which the covered entity becomes aware.

These new provisions are overly broad, and would require over-reporting of incidents to the Department, creating more work than utility. For example, as drafted under the Proposal, it would be a reportable cybersecurity event if an employee inappropriately shared login credentials to a privileged account with another employee to assist in carrying out an approved task. In such a case, even if the second employee only used the account once and for entirely approved purposes, because an employee gained unauthorized access to a privileged account it would be a reportable incident regardless of there being no risk to NPI as a result of the unauthorized access. Similarly, any cybersecurity event at a third party service provider that affects the covered entity, no matter how minor, would be a reportable cybersecurity event. Notably, the definition of a "cybersecurity event" in Part 500 is extremely broad, including unsuccessful attempts and events that have no impact on NPI. Requiring reporting of such cybersecurity events regardless of the materiality or impact of the event on the covered entity will result in significant over-reporting that serves no regulatory or practical purpose.

The Committee requests that the notifications for cybersecurity events at service providers and involving the compromise of a privileged account in the Proposal be amended to include a materiality threshold, or at a minimum, exclude technical and de minimis cybersecurity events.

Additionally, **Section 500.17(a)(2)** of the Proposal would require covered entities to provide "any information requested regarding the investigation of a cybersecurity event" to the Department within 90 days and would create a continuing obligation to update and supplement the information provided. We request that the requirement to provide all information requested by Department be limited to the information known. Also, the affirmative duty to update should be limited to material updates to the facts.

6. Transitional Periods Should be Extended

The Committee appreciates that the Proposal provides transitional periods to allow all covered entities time to come into compliance with new requirements. However, a number of requirements under the Proposal are subject to transitional periods that are insufficient to address the significant time and effort required to implement those new requirements in an enterprise setting. Accordingly, we request that the Proposal be revised to provide the following transitional periods to allow enough time for the planning, resource allocation, and implementation process to be carried out:

- Sections 500.7 (Access Privileges) and 500.12 (Multifactor Authentication) –2 years from the date of adoption.
- Section 500.13 (Asset Management and Data Retention Requirements) – 3 years from the date of adoption.
- Section 500.16 (Business Continuity and Disaster Recovery) – 1 year from the date of adoption for all requirements under 500.16.

7. Additional Requests for Clarification or Changes

In addition to the Committee's significant concerns regarding the Proposal outlined above, the Committee requests clarification on the following items:

- **Section 500.1 (c)** – As drafted, this definition of Class A Companies could be read such that any affiliate of a Class A Company would itself qualify as a Class A Company if it were located in New York, regardless of whether the affiliate meets the revenue threshold. Please clarify that while the revenue of affiliates counts toward a covered entity's revenue for purposes of the revenue threshold, affiliates that do not meet the threshold (or are not covered entities) do not themselves qualify as Class A companies.

- **Section 500.11(c)** – The Proposal would delete the limited exemption currently included in Section 500.11(c) of Part 500. It is unclear whether the deletion of this exemption is intended to enact a substantive change to the existing requirements. We request that the Department clarify that this provision was deleted as duplicative, and that individuals who previously relied on the limited exemption under 500.11(c) continue to be exempt under Section 500.19(b) and are not required to develop their own third party information security policy.

- **Section 500.16(d)** - The Proposal would require the CEO to be involved in annual incident response plan testing, regardless of whether the CEO would otherwise play a significant role in cybersecurity operations or incident response. Requiring the CEO's participation would not only be administratively difficult, but would also detract from the CEO's more strategic focus on risk management. We request that the language be amended to require that testing include all key staff that would be involved in an actual incident response scenario, including to the extent applicable, senior executives.

- **Appendix A** – The Proposal repeals Appendix A to Part 500, which currently defines the form of the required certification of compliance filed under Section 500.17(b). It is unclear whether the form of certification required under Part 500 will be modified, what form it will take, or if covered entities will be given more flexibility to draft their own certifications. We request clarification on whether the form of certification is anticipated to change and how. It is important that any revised form of certification that must be made in an individual capacity retain the "to the best of their knowledge" language to enable good faith certifications based on appropriate due diligence.

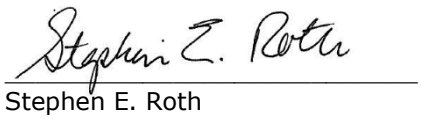
The Committee appreciates the time and resources the Department and its staff have devoted to this Proposal, as well as the opportunity to provide the Committee's views to the Department. We also appreciate the Department's careful consideration of the comments expressed herein. The Committee and its members stand ready to provide the Department with any information that may further your consideration of the concerns we have expressed and to engage in positive dialogue with the Department on these matters at your convenience.

Respectfully submitted,

FOR THE COMMITTEE OF ANNUITY INSURERS

Eversheds Sutherland (US) LLP

By:



Stephen E. Roth
Mary Jane Wilson-Bilik
Alexander F. L. Sand
Eversheds Sutherland (US) LLP

Cc: Justin Herring, Executive Deputy Superintendent, Cybersecurity Division

EVERSHEDS SUTHERLAND

From: Roth, Stephen <SteveRoth@eversheds-sutherland.us>
Sent: Wednesday, December 7, 2022 3:59 PM
To: CAI - Cyber Working Group <CAI-CyberWorkingGroup@eversheds-sutherland.us>
Cc: Committee of Annuity Insurers <CommitteeofAnnuityInsurers@eversheds-sutherland.us>; Wilson-Bilik, Mary Jane <mjwilson-bilik@eversheds-sutherland.com>; Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>
Subject: INPUT REQUESTED: Proposed CAI Comments on NYDFS' Proposed Amendment to its Cybersecurity Rule

This note follows-up on the November 17th call of the CAI's Cyber Working Group during which we discussed areas of possible comment on NYDFS' proposed amendments ("Proposal") to its Cybersecurity Requirements for Financial Services Companies (23 NYCRR Part 500) (the "Cyber Reg").

The purpose of this note is to set forth our thoughts and recommendations regarding those issues that the Committee would comment upon, and to solicit input from Committee members on those or other issues that members believe the Committee should comment on. We are looking for your input by no later than next Tuesday, December 13 so that we can prepare a draft comment letter for review by the Committee's Cyber Working Group.

Background

NYDFS published the Proposal on November 9, 2022, with comments due by **January 9, 2023**. The Proposal includes several significant changes to the Cyber Reg., some of which are consistent with guidance previously published by NY DFS, and some of which represent entirely new concepts, as discussed in previous emails.

Issues for Potential Comment

Based on the November 17 discussion of the CAI Cyber Working Group, below is a list of issues for comment by the Committee arranged in order of significance. We welcome feedback on our list and commentary.

1. *Inappropriate Board and CEO Requirements*

The Proposal includes several provisions that place burdensome and arguably inappropriate duties on the Board and CEO with respect to cybersecurity:

- **Section 500.4(d) – Cybersecurity Governance – Board Duties**. The Proposal would require Boards (and equivalent bodies) to "exercise oversight of, and provide direction to management on, the covered entity's cybersecurity risk management." The Proposal would also require the Board "to have sufficient expertise and knowledge, or be advised by persons with sufficient expertise and knowledge, to exercise effective oversight of cybersecurity risk management."

The requirement to "provide direction to management" in particular oversteps the role of the Board by pushing them into a managerial role. We would suggest language to clarify or reframe this requirement in ways more appropriate to the Board's role. This theme also plays out through additional new requirements proposed under Sections 500.3 (Board approval of cybersecurity policies) and 500.5 (timely notice to Board of material cybersecurity issues).

Similarly, the Proposal would require the CEO to be involved in annual incident response plan testing, regardless of whether the CEO would otherwise play a significant role in cybersecurity operations or incident response.

- **500.16(d)** - CEO required to participate in annual incident response plan testing.

We would propose language that would provide more flexibility for covered entities to define how they set up their cybersecurity programs and who plays what role.

2. *Strict Standard for Compliance Certification*

The Proposal provides Covered Entities with the ability to file a certificate of non-compliance, a needed alternative to the current mandated certification of compliance. However, the standard for filing a certification of non-compliance is overly rigid.

- **Section 500.17(b) – Certification of compliance**. This Section would require a Covered Entity to file an acknowledgement of non-compliance any time the entity "did not fully comply with all requirements" of the Cyber Reg. When paired with the Proposal's new definition of a "violation" of the Cyber Reg. that includes non-compliance for any 24-hour period, even minor and non-material gaps in compliance could prevent covered entities from filing a certificate of compliance.

We would propose amended language that would clarify that routine gaps in compliance that are identified and corrected through normal compliance procedures would not prevent a Covered Entity from filing a certificate of compliance.

3. *Annual External Audit Requirement*

The Proposal would require Class A companies to annually hire external auditors to audit their cybersecurity program.

- **Section 500.2(c) – Independent Audit.** This Section would require Class A companies to conduct an "independent audit of their cybersecurity programs at least annually". "Independent audit" would be defined as an audit "conducted by external auditors…."

This external audit requirement is different from the pre-proposal, which would have allowed an independent internal audit function to satisfy this requirement. Requiring an external audit annually is an overly burdensome obligation that serves limited purpose for a cybersecurity program that will not change drastically year to year. We would propose that an independent internal audit should be allowed and, at minimum, the frequency of the external audit be decreased to align with the 3-year external penetration testing requirement.

4. *Overly Rigid Cybersecurity Event Notice Requirements*

The Proposal expands the existing requirements to notify NYDFS of cybersecurity events to require notice of any compromise of a privileged account or event affecting a service provider regardless of materiality, and creates strict affirmative requirements around how reporting is made.

- **Section 500.17(a)(1)(iii) – Notice of compromise of privileged account.** This new provision would require covered entities to notify NYDFS of any cybersecurity incident that involves compromise of a privileged account (i.e. any account with elevated permissions that can be used for security-relevant functions or affect material system changes). It does not provide any materiality qualifier or account for a de-minimus/technical type of compromise.

- **Section 500.17(a)(2) – 90 Days to provide information on incident.** This provision would require covered entities to provide "any information requested regarding the investigation of a cybersecurity event" and creates a continuing obligation to update and supplement the information provided.

- **Section 500.17(a)(3) – Notice of all service provider cybersecurity events.** Similar to the notice requirement for compromised privileged accounts, the Proposal would require covered entities to notify the NYDFS of any cybersecurity event at a third party service provider of which the covered entity becomes aware.

These new provisions are overly broad, and would require over-reporting of incidents to NYDFS, creating more work than utility. We would propose that the notifications for cybersecurity events at service providers and involving the compromise of a privileged account be amended to include a materiality threshold. Additionally, the requirement to provide all information requested by NYDFS should be limited to the information known, and the affirmative duty to update should have some identified limit after which updating is no longer required (e.g. after all material facts have been provided).

5. Possible Sources of Technical Challenges

The Proposal contains several new requirements that may pose technical challenges. ***To the extent feasible, we request that interested Committee members seek high-level feedback from internal IT and security teams on whether the following requirements are practically feasible or reasonable and to share that feedback with us. We would include comments in the CAI comment letter based on that feedback.***

- **Section 500.5(a)(2) – Manual Review of some systems to assess for vulnerabilities**. The proposal would require any system not subject to automatic vulnerability scans to be manually reviewed for vulnerabilities at a frequency informed by the risk assessment.

- **Section 500.7(b) – Require PAM and password blocking for all user accounts.** This section would require Class A Companies to implement a privileged access management solution and automated blocking of commonly used passwords for all user accounts.

- **Section 500.12 (b) – Multi-factor authentication for services accounts.** The Proposal would require MFA to be applied to all privileged accounts including service accounts. Under the pre-proposed version, an exemption was provided for service accounts.

Please let us know by next Tuesday, December 13, if you have any questions or concerns with the Committee commenting on the issues summarized above. Similarly, if there are other issues you believe that the Committee also should comment on, please let us know those issues. We intend to reach out to LICONY at the appropriate time to let them know that the Committee will be commenting and to coordinate with LICONY in whatever manner will be most effective. Please contact Al Sand (512-721-2721), Mary Jane Wilson-Bilik (202-383-0660) or myself with your thoughts.

Regards,

Steve

Stephen E. Roth | Partner | T: +1.202.383.0158

EVERSHEDS SUTHERLAND

From: Roth, Stephen
Sent: Wednesday, November 2, 2022 11:26 AM
To: CAI - Cyber Working Group <CAI-CyberWorkingGroup@eversheds-sutherland.us>
Cc: Wilson-Bilik, Mary Jane <mjwilson-bilik@eversheds-sutherland.com>; Sand, Alexander <AlexanderF.L.Sand@eversheds-sutherland.us>
Subject: Possible CAI Comments on NYDFS' Proposed Amendment to its Cybersecurity Rule

Since the last meeting of the CAI's Cybersecurity Working Group, New York's Department of Financial Services ("NYDFS") released a pre-proposed draft second amendment to its Part 500 cybersecurity rule (the "Cyber Rule") (attached). After a brief comment period that ended in late August, NYDFS has indicated that it is now poised to officially release a formal proposal to amend its Cyber Rule. A 60-day public comment period would begin once the proposal is published in the NYS Register.

We believe that the NYDFS is embarking on a new era of cybersecurity regulation for the financial services industry that will result in a more stringent regulatory atmosphere in New York. The proposed amendment is expected to elevate cybersecurity requirements for large companies, increase Board and C-suite responsibility and accountability, expand breach notification obligations, augment risk assessment requirements, and establish specific business continuity and disaster recovery requirements.

It is anticipated that the proposed second amendment will implement some significant changes to the Cyber Rule, the most notable of which are:

1. Permitting a new "acknowledgement of non-compliance" filing, which should prevent the Catch-22 some companies experience in not being able to certify to full compliance, but which creates new risks for Covered Entities.
2. Requiring Boards of Directors to have or obtain cybersecurity expertise and knowledge "sufficient to effectively oversee cybersecurity risk."
3. Requiring that CISOs have "adequate independence and authority."
4. Expanding existing breach notification obligations and requiring 24-hour reporting and justification of ransom or extortion payments.
5. Creating a separate class of larger Covered Entities called "Class A" companies, which are companies with over 2,000 employees or over $1 billion in gross annual revenue over the last three fiscal years from all business operations of the company and all its affiliates, and subjecting them to even more stringent cybersecurity requirements and scrutiny.
6. Increasing emphasis on senior officer responsibility and accountability for cybersecurity, including requiring the CEO to personally certify compliance.
7. Augmenting risk assessment requirements, particularly for inventorying data and assets.
8. Mandating specific content requirements for a business continuity and disaster recovery plan.
9. Defining failure to meet any requirement of the regulations for 24-hours as a violation potentially subject to enforcement by NYDFS.

While we wait to see what the DFS finally proposes, it seems highly likely that some of the new Cyber Rule requirements could pose challenges for Committee members and overlap in difficult ways with, or potentially conflict with, the SEC's newly proposed cybersecurity rules, creating even more regulatory burden on companies. For this reason, we are planning to convene a meeting of the CAI Cyber Working Group either next week, or if the proposed amendment has not been released by then, the following week to discuss the proposed amended Cyber Rule and

EVERSHEDS SUTHERLAND

whether Committee members believe it would be helpful for the Committee to prepare and submit a comment letter on what is published in the NYS Register.

If you have any questions in the meantime, or thoughts about particularly problematic aspects of what the DFS released in its pre-proposal, please reach out to Mary Jane Wilson-Bilik, Al Sand or myself.

Steve