North American
CRO Council

DRAFT V.1

November 11, 2016

Maria T. Vullo, Superintendent of Financial Services
New York State Department of Financial Services
One State Street
New York, NY 10004-1511
Via e-mail: CyberRegComments@dfs.ny.gov

Comment Submission on Proposed 23 NYCRR 500 – Cybersecurity Requirements for Financial Services Companies

Dear Superintendent Vullo,

The North American CRO Council ("CRO Council" or "Council") appreciates the opportunity to comment on the Proposed New York Cybersecurity Requirements for Financial Services Companies ("Proposed Regulation"). The CRO Council is a professional association of Chief Risk Officers ("CROs") from leading insurers based in the United States, Canada, and Bermuda. Member CROs currently represent 29 of the largest Life, and Property and Casualty insurers in North America. As a body formed to promote sound practices in risk management, the CRO Council appreciates the opportunity to submit its comments and concerns regarding the Proposed Regulation.

The CRO Council strongly supports the goal of the Proposed Regulation, described in the Proposed Regulation's Introduction, Section 500.0: "Given the seriousness of the issue and the risk to all regulated entities, certain regulatory minimum standards are warranted, while not being overly prescriptive so that cybersecurity programs can match the relevant risks and keep pace with technological advances. Accordingly, this regulation is designed to promote the protection of customer information as well as the information technology systems of regulated entities. This regulation requires each company to assess its specific risk profile and design a program that addresses its risk in a robust fashion. . ."

The CRO Council believes cybersecurity is an essential element of an insurance company's enterprise risk management processes and is supportive of risk-based, practical approaches to managing cybersecurity risk via cybersecurity frameworks that allow each insurer to take into account the broad security environment in which it operates, the nature, scale, complexity and risk profile of its operations, the sensitivity of the information it maintains, and the security laws and regulations to which it is already subject. Uniformity of regulatory approaches to cybersecurity requirements is essential to ensuring the effective and efficient management of an insurer's information security program. The complexity of having to comply with differing and often conflicting state laws only adds risk to the important task of managing cybersecurity threats. As currently drafted, the Proposed Regulation is problematic with regard to these principles. Moreover, by imposing prescriptive standards, rather than taking a true, risk-based approach to security, the proposed regulation may actually increase the risk of a successful cybersecurity event by diverting limited security resources from more urgent and higher leverage activities.

The Proposed Regulation Does Not Promote a Uniform Risk-Based Approach to Cybersecurity

Other key existing security frameworks, such as the National Institute of Standards and Technology (NIST), Gramm Leach Bliley Act (GLBA), and Health Insurance Portability and Accountability Act (HIPAA) are focused on active risk management rather than rigid, prescriptive security requirements. The Proposed Regulation, in deviating from the risk-based approach of other key security frameworks, undercuts the goal of uniformity. Uniform security standards that are risk-based, flexible and appropriate to the nature, size and complexity of an insurer are essential to ensuring the effective and efficient management of an insurer's information security program. The complexity of having to comply with differing and often conflicting state and federal laws only adds risk to the important task of managing cybersecurity threats. Furthermore, a prescriptive approach is not in alignment with the rapid evolution of threats and control technologies and approaches that is characteristic of the cybersecurity space. The Council believes that a consistent, risk-based and uniform state approach to cybersecurity regulations is essential and urges state regulator collaboration to achieve this goal.

The Definitions of Key Terms are Overly Broad and Don't Include a Materiality Standard or Harm Trigger

The definitions of key terms that underlie the Proposed Regulation's requirement are overly broad. Specifically, the definition of "Information Systems" and "Nonpublic Information" include information and systems that are not sensitive, and the unauthorized access, disruption or use of which is unlikely to lead to material harm to the subject. Certain measures and controls prescribed by the Proposed Regulation may only be appropriate for sensitive information or high risk systems with sensitive information. Accordingly, the Council urges that the Proposed Regulation incorporate the concept of Sensitive Nonpublic Information and Sensitive Information Systems, focusing on data elements and systems that, if compromised, could create a material risk of fraud. Further, the definition of "Cybersecurity Event" is not limited to acts likely to result in material risk of harm and reporting of such occurrences would overburden resources of Covered Entities and the Department of Financial Services without providing commensurate benefit. Accordingly, this definition should incorporate the concept of malicious acts that result in a material adverse impact to the business, operations or security of the Covered Entity or material risk of identity theft or fraud to the subject of the Sensitive Nonpublic Information.

Risk-Based, Practical Approaches to Managing Cybersecurity Risk

Notwithstanding the statements in the Proposed Regulation's Introduction quoted above, many of the actual requirements of the Proposed Regulation are prescriptive and not risk-based. The Council believes it is important, given the evolving nature of this risk and how it is managed, to avoid a highly prescriptive approach to managing cybersecurity risk. Many facets of the Proposed Regulation mandate specific security protections. As technology evolves, alternative methods for mitigating risk likely will be developed and may prove to be better alternatives for companies to use in light of their exposure and security protocols. The following provide some examples of areas where we feel the Proposed Regulation is too prescriptive and why.

Section 500.15 requires encryption of all of an insurer's Nonpublic Information both in transit and at rest (within a one and five year transition period, respectively). Given the breadth of the current definition of Nonpublic Information, which essentially includes any information, this requirement is neither risk-based nor practical. This requirement should be targeted to sensitive information, and while encryption in

transit can be useful, encryption of information stored on an insurer's networks comes with serious limitations, including extreme cost and significant disruption of normal business operations. Further, encryption is but one means of protecting sensitive data, and it should not be perceived a panacea. Many forms of encryption have exploitable vulnerabilities, and sophisticated hackers have found alternative means around even advanced forms of encryption. For example, simply obtaining an authorized user's password, commonly done through "phishing" or other techniques, will defeat even the most secure encryption. Other means of protecting sensitive data at rest may be more effective for an insurer to implement and regulators should avoid mandating a specific technological response. The Council advocates for a comprehensive, flexible approach to protection of sensitive data stored on networks and systems, to include access, logging, monitoring and detection controls, and data loss prevention, as opposed to one specific means of protecting data.

The Council is supportive of a risk-based approach to the management of third party service provider risk, which includes exercising appropriate due diligence in the selection process, contractual security requirements appropriate to the sensitivity of the information to which the third party has access, and appropriate ongoing oversight of the third party. Section 500.11 as currently drafted is overly prescriptive. Again, the sensitivity of the information is not taken into consideration, nor is it practical (given the thousands of vendors that large organizations may use and the contractual nature of these relationships) to require an annual assessment of every third party service provider regardless of the risk assessment of that particular vendor.

Section 500.12 broadly requires multi-factor authentication without regard to the sensitivity of the systems, networks or the data therein. While multi-factor authentication may be prudent and effective for certain systems and networks, the Proposed Regulation's broad application is not risk-based or practical. The Council believes that a risk-based approach should be utilized to determine those circumstances in which multi-factor authentication is appropriate for access to sensitive information and in consideration of the entire control environment.

The Council urges modifications to the Proposed Regulation such that the required cybersecurity program, policies and procedures are risk-based and practical, which means they not be overly prescriptive but rather tailored to the nature, scale, complexity and risk profile of the Covered Entity's operations, the sensitivity of the information it maintains, and take into account the broad security environment in which it operates.

Confidentiality Concerns

The reports contemplated under Section 500.04(b) would likely contain highly sensitive information that should not be exposed to potential public disclosure under the Public Officers Law (FOIL) or through a cybersecurity event at the Department. Therefore, it is critical that any reports made available to the superintendent under Section 500.04(b) should be returned to the Covered Entity after review and not retained on Department systems.

Notice of Cybersecurity Event Must Not Detract from Risk Mitigation Efforts

The superintendent notification requirements in Section 500.17 are concerning from the standpoint that in the event of a breach a Covered Entity's immediate focus needs to be on conducting its investigation and securing its systems and information from any further breach. The requirement of providing notice

North American
CRO Council

to the superintendent of a cybersecurity event within 72 hours may not be practical and may actually detract from the Covered Entity's investigation and risk mitigation efforts. The Council asks that a more practical and workable approach be taken in Section 500.17 that permits a Covered Entity to appropriately focus its investigation and threat mitigation efforts in the event of a cybersecurity breach, while still engaging the superintendent as soon as practically possible following a breach. Furthermore, as stated above in several instances, the breadth of the definition of Nonpublic Information makes this reporting obligation neither risk-based nor practical.

The CRO Council appreciates the opportunity to provide our comments and concerns on the Proposed Regulation. In the event that the Superintendent enacts the Proposed Regulation with a prescriptive approach that mandates specific security protections, such as encryption of data at rest and multi-factor authentication regardless of the sensitivity of the systems, networks or the data therein, then the Council urges that a reasonable transitional period, of no less than one year, be permitted given the cost and complexity to comply with such requirements.

Sincerely,

Stephen Gruppo, Chair
North American CRO Council

Tammy Roou, Chair
CRO Council Cyber Risk Working Group