NAMIC®
NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

Where the future of insurance has its voice®

3601 Vincennes Road, Indianapolis, Indiana 46268
Phone: 317.875.5250 | Fax: 317.879.8408

www.namic.org

122 C Street N.W., Suite 540, Washington, D.C. 20001
Phone: 202.628.1558 | Fax: 202.628.1601

November 14, 2016

Cassandra Lentchner, DFS Deputy Superintendent for Compliance
New York Department of Financial Services
One State Street, New York, NY 10004-1511

Re: Cybersecurity Requirements for Financial Services Companies
Proposed Regulation 23 NYCRR 5000

Dear Deputy Superintendent Lentchner:

On behalf of National Association of Mutual Insurance Companies (NAMIC)[1] members, I am writing regarding the proposed regulation on Cybersecurity Requirements for Financial Services Companies ("Proposal"). NAMIC's concerns with the Proposal centers around several broad themes: the specificity of the security requirements not allowing risk-based approaches and flexible solutions, the breadth of the applicable data and requirements, the extremely tight implementation schedule, the questions of confusion with existing laws and with confidentiality, and the significant increase in compliance costs where some of the requirements may be infeasible.

Recognizing that DFS understandably seeks to bolster cybersecurity protections for New York financial institutions and their customers, NAMIC asks DFS to consider using workable risked-focused ways of achieving that goal. In this letter NAMIC walks though observations about each Section through the lens of increasing the ways DFS could take a risk-based approach that allows for some flexibility in implementation – NAMIC's intent is to offer thoughts to DFS based on the design of the regulation articulated in the introduction to the Proposal and on the importance of those concepts in NAMIC members' approach to cyber issues.

Given the Proposal's significant impact on Covered Entities, NAMIC strongly urges DFS not to promulgate a final regulation without providing interested parties an opportunity to review and comment on the effect any revised wording would have on their customers, operations and security.

Before turning to Section-by-Section notes, NAMIC would like to underscore the fact that cyber risks and cybersecurity need not be considered in a vacuum because they are part of a continuing and evolving area of privacy protections (including a wide-range of internal measures as well as legal protections and regulatory requirements) to protect consumers and financial services entities from criminal activity. While "cybersecurity" – perhaps loosely defined as measures taken to protect computer networks against unauthorized use or attack – may feel new, much of the foundation for dealing with these concerns is already in place. For example: the existing privacy landscape countrywide[2] and in New York[3] requires that financial services entities maintain a risk-based comprehensive written information security program containing administrative, technical and physical safeguards to protect the security and confidentiality of consumers' nonpublic personal informational. Also, businesses experiencing a breach – a cyber event – are subject to a New York law that outlines their appropriate response.[4]

[1] NAMIC is the largest property/casualty trade association in the country, serving regional and local mutual insurance companies on main streets across America as well as many of the country's largest national insurers. NAMIC consists of more than 1,300 property/casualty insurance companies serving more than 135 million auto, home and business policyholders, with more than $208 billion in premiums accounting for 48 percent of the automobile/homeowners market and 33 percent of the business insurance market nationwide. In New York, NAMIC members write about 60% of the auto insurance market.

[2] See Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801, et. seq.) and Standards for Safeguarding Customer Information Model Regulation (NAIC 2002). For the years since the Gramm-Leach-Bliley Act, DFS and other financial services regulators around the country have had standards in place for their regulated entities to safeguard customer information.

[3] See New York Insurance Department Regulation 173 (11 NYCRR 421) and Circular Letter No.7 (February 3, 2000).

[4] See New York General Business Law Sec. 899-aa.

INTRODUCTION – Section 500.0

The New York State Department of Financial Services ("DFS") has been closely monitoring the ever-growing threat posed to information and financial systems by nation-states, terrorist organizations and independent criminal actors. Recently, cybercriminals have sought to exploit technological vulnerabilities to gain access to sensitive electronic data. Cybercriminals can cause significant financial losses for DFS regulated entities as well as for New York consumers whose private information may be revealed and/or stolen for illicit purposes. The financial services industry is a significant target of cyber threats. DFS appreciates that many firms have proactively increased their cybersecurity programs with great success.

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 risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations. A regulated entity's cybersecurity program must ensure the safety and soundness of the institution and protect its customers.

It is critical for all regulated institutions that have not yet done so to move swiftly and urgently to adopt a cybersecurity program and for all regulated entities to be subject to minimum standards with respect to their programs. The number of cyber events has been steadily increasing and estimates of potential risk to our financial services industry are stark. Adoption of the program outlined in these regulations is a priority for New York State.

In highlighted sentences, DFS articulates a reasonable and balanced way to design a cybersecurity regulatory framework to protect customer information while allowing entities to match relevant risk and keep pace with technological changes. NAMIC favors this approach and would like to explore ways DFS could incorporate it throughout the Proposal, explicitly connecting certain cybersecurity program measures to relevant risks in a way that is not overly prescriptive.

Risk-Based:

- Matching controls to relevant risks presumes being able to differentiate between risks and risk levels based on potential for causing material problems. Throughout this letter NAMIC aims to encourage this differentiation and to ask DFS to avoid a one-size-fits-all approach.

- Inserting additional background information – about the objectives of cybersecurity program standards, about various guidelines and resources, and about existing laws – may guide financial institutions seeking to comply with the Proposal. For example:

    - Consistent with today's financial examination approach and drawing on high-level concepts, it may be useful to explain that standards in the regulation are expected to direct financial institutions in particular categories of activity: (1) identification: devoting resources to the identification of cybersecurity risks and conduct a cybersecurity risk assessment process that includes appropriate technical expertise and appropriate management and/or board involvement; (2) prevention: having a prevention strategy that considers (i) a combination of risk-based policies, system and network access controls, and data security protection appropriate to the operating environment, including volume and type of sensitive information obtained, maintained or transmitted, applicable security laws and regulations, the size and complexity of the entity, and nature and scope of its activities; (ii) risks presented by third-party access to network information; and (iii) employee training appropriate to the risk associated with that employee's assigned responsibilities; (3) detection: having detective controls (which may include things like penetration testing, network monitoring, vulnerability assessments and authentication as appropriate); and (4) response and recovery: requiring an incident response plan that may leverage concepts from an entity's broader disaster recovery plan and regulator notice.

      While these underlined purpose categories are included in the cybersecurity policy design requirement in Section 500.02(b), from there they are not then structurally linked to each of the Proposal's substantive provisions in a way that outlines a mandatory purpose standard and then allows for examples of ways it could be accomplished adapt over time to account for changes in technology and the ever-changing cybersecurity threat landscape. Cyber actors deploy tactics that may change and particular firms may face unique exposures that may change over time. Firms must

be flexible in their approach and resources to combat such threats. Successful cybersecurity measures must be constructed to address the ever-evolving risks faced by each of the different types of financial firms based on size, resources, and risk exposure.

- In developing cybersecurity programs, processes and procedures, financial entities may draw on expertise from a number of resources including standard organizations like the National Institute of Standards and Technology (NIST) Cybersecurity Framework as well as from comprehensive regulations from federal agencies (such as the Interagency Guidelines).

  If using the underlined purposes as a way to organize a regulation, DFS could further point to these standards as additional non-exclusive examples of ways to meet the requirements.

Flexible:

- The flexible approach sketched above may allow for a more efficient use of resources, for prioritizing risks and for deciding the best ways to mitigate identified risks or to implement other controls. Throughout the Proposal, flexibility may be increased consistently in a few ways, including use of a reasonability standard or outlining principles (in place of a mandate) and then allowing for alternatives through examples that may serve as helpful guidance, but that do not preclude other methods; or a safe harbor or a compliance deemer for certain approaches. Flexibility may provide for a more long-standing framework given technological and other changes.

- Because the word “ensure” at the end of the second paragraph may imply absolute certainty, kindly consider “take reasonable steps to preserve” in its place.

SCOPE & DEFINITIONS – Section 500.01

NAMIC implores DFS to narrow definitions to focus on the most at-risk data, systems, etc. Refining the definitions may have a significant salutary impact on several of the concerns with the substantive provisions.

Risk-Based: NAMIC also encourages DFS to draft a few additional definitions to better tailor the scope of the requirements. Specifically, please consider:

- Adding Sensitive Nonpublic Information as well as Sensitive Information Systems in order to differentiate between different levels of sensitivity of data and systems. Understanding these differences may prove essential to entities looking to think about the risk posed by different data and systems.

- Defining a narrower Cybersecurity Incident to follow materiality triggers more consistent with the breach law (or revising Cybersecurity Event along these lines).

- Including a Third Party Service Provider definition (to exclude other DFS regulated entities (including independent agents)).

(a) ***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.

Flexible: By amending the Covered Entity definition, DFS may be able to address many practical questions and concerns. For example, please consider:

- Allowing for related entities to comply with the requirements on a consolidated basis as appropriate rather than separately by entity. Given that cybersecurity support is often done at an enterprise level, rather than clarifying permitted flexibility each time the term Covered Entity is used, consider whether to amend the definition to make it clear that within a group a parent or an affiliate may act on behalf of or provide resources to the entity. Consider a similar issue for captive agents, which serve as an example of entities needing flexibility with respect to how they structure ownership, use, maintenance and other responsibilities for systems and procedures.

- Clarifying that this relates to New York DFS regulated entities.

- Using a different term because “Covered Entity” is already a critically important defined term of art in privacy compliance for those subject to HIPAA.

- Specifying that no Covered Entity under the Proposal need be considered a third party by another Covered Entity. Presumably in assessing risk a Covered Entity should be able to consider the legal and regulatory mandates to which a third party is subject and to the extent an entity is already subject to these requirements in its own right, another Covered Entity should be able to rely on the third party engaging in the procedures outlined in the Proposal.

(d) ***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.

Risk-Based:

- NAMIC strongly urges DFS to frame this definition as a Cybersecurity Incident to be more consistent with understood terminology and focus on material adverse impact to particularly sensitive nonpublic information and to particularly sensitive information systems. As drafted, the Proposals broad definition of Cybersecurity Event will prompt what may be costly and busy administrative work without resulting meaningful cybersecurity protections.

- NAMIC urges DFS to remove references to "unsuccessful" and "attempt" from the Proposal. A significant number of unsuccessful attempts occur daily for each entity.[5]

- NAMIC urges DFS to include a material risk of harm component. Some flagged attempts occur as a result of harmless human error (for example, when a customer enters an incorrect password or other credential). Depending on circumstances, there can be situations in which information is accessed but there is no threat of material harm such as when the nonpublic information cannot be read (because of encryption or other technological safeguard). Existing laws and regulations may be instructive on how to define a material risk. For example, the definition of a data breach under New York's General Business law provides: "unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business."[6] Conflicting definitions and standards may complicate rather than expedite or enhance incident response.

- As drafted, there is no link between an event and sensitive Nonpublic Information for New York residents. Rather, the Proposal appears to sweep in all information stored on an Information System.

- Incorporating the broad scope of the Information System (which includes electronic things like telephone switching) makes this definition problematic. To be more risk-based, it should be limited to information on a computer network.

[5] One way that entities may opt to keep track of threats is by sharing information about cyber security threats. For example, the Financial Services Information Sharing and Analysis Center (FS-ISAC) – sponsored by the U.S. Department of Treasury – is one mechanism for getting information quickly to guard against cyber threats. Perhaps they have and would be willing to share information on the volume of unsuccessful attempts with DFS.

[6] See New York General Business Law Section 899-aa(1)(c).

(e) ***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.

Risk-Based:

- NAMIC recommends DFS amend this definition in order to limit it to those systems containing the particular kind of data it seeks to protect. As discussed elsewhere, the greatest cyber risks are with the Nonpublic Information that is most sensitive.

- NAMIC encourages DFS to revise this definition to focus where the risk is greatest, on things like use of "organized computer systems for the collection, storage and processing of sensitive nonpublic information, rather than on "electronic information resources," which appears to be very broad and may sweep in things beyond computers. Such a broad definition may divert resources from cyber protections that will be more impactful.

(f) ***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; or
2. Possession factors, such as a token or text message on a mobile phone; or
3. Inherence factors, such as a biometric characteristic.

Risk-Based:

- Consistent with the discussion about authentication procedures, to allow for a tailored approach for the risk, consider framing this overall issue as "authentication" and then having the multi-factor definition for the more limited instances when particularly sensitive information may be accessed.

- To the extent this is considered a menu and that at least two of the numbered items under (f) must be used, please consider: expanding (1) to also include a user name, and adding another set of knowledge factors to account for things like challenge questions. Depending on the Covered Entity's risk assessment, it may be appropriate to satisfy the two-type requirement through the use of a user name and password along with answering a challenge question.

- The Multi-Factor Authentication definition may imply that factors must come from different categories (knowledge, possession and inherence). If an entity reviews the risk and determines that two pieces of authentication from one category would suffice, it should be permissible.

(f) ***Nonpublic Information*** shall mean all electronic information that is not Publicly Available Information and is: (1) Any 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 that an individual provides to a Covered Entity in connection with the seeking or obtaining of any financial product or service from the Covered Entity, or is about an individual resulting from a transaction involving a financial product or service between a Covered Entity and an individual, or a Covered Entity otherwise obtains about an individual in connection with providing a financial product or service to that individual; (3) Any information, except age or gender, that is created by, derived or obtained from a health care provider or an individual and that relates to the past, present or future physical, mental or behavioral health or condition of any individual or a member of the individual's family or household, or from the provision of health care to any individual, or from payment for the provision of health care to any individual; (4) Any information that can be used to distinguish or trace an individual's identity, including but not limited to an individual's name, social security number, date and place of birth, mother's maiden name, biometric records, any information that is linked or linkable to an individual, including but not limited to medical, educational, financial, occupational or employment information, information about an individual used for marketing purposes or any password or other authentication factor.

Risk-Based:

- NAMIC strongly urges DFS to amend this definition to narrow the scope to the types of customer information (particularly sensitive information) that are the greatest threat. The use of "all" and "any" cause concern.

- The concept that the Proposal's requirements should apply equally to all electronic information that is not Publicly Available Information – regardless of the risk and sensitivity – is extremely broad (and potentially inconsistent with existing definitions).

- NAMIC asks that this definition be limited to customer data and not include a Covered Entity's business related information. Not only do the objectives differ from a regulation "designed to promote the protection of customer information," but considerations of business information may more commonly be in a business continuity plan or in another governance project. DFS also may consider these protections through their financial examinations. To the extent that DFS must include business information, NAMIC encourages DFS to do so in a different definition so that all involved can think through the handling and types of trade secret business data (the release of which would materially impact the entity) separately from the risks related to sensitive customer information to which the entity has other legal obligations.

- Nonpublic Information is the framework here as well as in other New York laws. Such a broad definition may hinder prioritization of risks, which is a critical aspect of effective risk management and corporate governance.

(j) ***Publicly Available Information*** means all 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 subsection, 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) That the information is of the type that is available to the general public; and (ii) 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.

Risk-Based:

Operationally, it would be impracticable for a Covered Entity to affirmatively and subjectively confirm whether an individual has requested that some particular unknown piece of public information be considered private (as outlined in (j)(1)(ii)). Also, consistent with applicable risk management policies and procedures, Covered Entities need to be able to categorize with certainty the level of sensitivity associated with different pieces of customer data.

CYBERSECURITY PROGRAM [ESTABLISH & MAINTAIN] - Section 500.02(a)

(a) Cybersecurity Program. Each Covered Entity shall establish and maintain a cybersecurity program designed to ensure the confidentiality, integrity and availability of the Covered Entity's Information Systems.

Risk-Based:

- To reflect a risk-based approach, additional language could be inserted to indicate that such cybersecurity program should be appropriate to the entity's size and complexity, the nature and scope of its activities and the sensitivity of the Nonpublic Information it holds.

- Because the word "ensure" may imply absolute certainty, kindly consider "protect" in its place.

Flexible:

- To avoid duplicate administrative work without additional security benefit, because of the reference to "each Covered Entity," please clarify that nothing in the regulation precludes an entity within a group from using the cybersecurity program of an affiliated entity to the extent that those related entities are covered under the same cybersecurity program (for example, consider a parent and its subsidiary).

- To the extent an entity already has a cybersecurity program as part of its risk-based comprehensive written information security program with administrative, technical and physical safeguards as required under Regulation 173 implementing Gramm-Leach-Bliley, or any other law or regulation, it may be helpful to indicate how to specifically refer to revisions to existing programs, if such revisions are needed. Is would also be helpful for DFS to confirm that nothing here mandates a separate policy if cybersecurity risks are addressed under existing policies or that nothing precludes including a cybersecurity program as a component of that or any other program at the entity.

CYBERSECURITY PROGRAM [DESIGN] - Section 500.02(b)

(b) The cybersecurity program shall be designed to perform the following core cybersecurity functions:
(1) identify internal and external cyber risks by, at a minimum, identifying the Nonpublic Information stored on the Covered Entity's Information Systems, the sensitivity of such Nonpublic Information, and how and by whom such Nonpublic Information may be accessed;
(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 all regulatory reporting obligations.

Risk-Based:

- The Proposal appears to impose a potentially overwhelmingly vast set of projects under (b)(1) to identify information location, type and access (using the broad definitions of Information Systems and Nonpublic Information) regardless of the level of threat. Without a risk-based approach, an entity cannot prioritize more meaningful cyber controls and direct attention to the greatest threats. Narrowing the scope would aid in directing attention and resources to particularly sensitive Nonpublic Information and Information Systems as well as to more material Cybersecurity Incidents, rather than an unworkable broader Cybersecurity Event as outlined in the Proposal.

- To reflect a risk-based approach, wording could be revised, perhaps by inserting reasonableness and materiality (consider "reasonably designed" in (b) and "reasonably foreseeable material internal and external cyber risks" in (b)(1)) as well as appropriateness ("the following core cyber security functions, as appropriate" in (b) and "to mitigate [removing "any"] negative effects as appropriate" in (b)(4)).

Flexible:

- To leverage the flexibility of the existing framework, refer to the same "administrative, technical and physical safeguards" wording in (b)(2) (in place of "defensive infrastructure and the implementation of policies and procedures").

- For efficiency, the cybersecurity program should be explicitly permitted to draw upon and refer to a variety of the Covered Entity's resources. For example, it may be relevant for an entity to point to its existing breach or incident response plan, its business continuity plan, or other applicable processes and procedures.

CYBERSECURITY POLICY [POLICY CONTENT] - Section 500.03

(a) Cybersecurity Policy. Each Covered Entity shall implement and maintain a written cybersecurity policy setting forth the Covered Entity's policies and procedures for the protection of its Information Systems and Nonpublic Information stored on those Information Systems. The cybersecurity policy shall address, at a minimum, the following areas: (1) information security; (2) data governance and classification; (3) access controls and identity management; (4) business continuity and disaster recovery planning and resources; (5) capacity and performance planning; (6) systems operations and availability concerns; (7) systems and network security; (8) systems and network monitoring; (9) systems and application development and quality assurance; (10) physical security and environmental controls; (11) customer data privacy; (12) vendor and third-party service provider management; (13) risk assessment; and (14) incident response.

***Risk-Based*:**

- To reflect a risk-based approach, the wording related to the cybersecurity policy could be expanded in the first line to indicate that such cybersecurity policy should be appropriate to the entity's size and complexity, the nature and scope of its activities and the sensitivity of the Nonpublic Information.

- Consider removing (5), capacity and performance planning, as it is not relevant to the risk of disclosing non-public information.

Flexible:

- To avoid duplicate administrative work without additional security benefit, because of the reference to "each Covered Entity," please clarify that nothing in the regulation precludes an entity within a group from using the cybersecurity program of an affiliated entity to the extent that those related entities are covered under the same cybersecurity program (for example, consider a parent and its subsidiary).

- The level of detail shown on the list may be a challenge for some smaller entities. If including this list under (a), please consider:

    - The existing financial services' Standards for Safeguarding Customer Information, the subject of Regulation 173, may be a helpful resource in a number of ways. First, the framework of the Information Security Program is explicitly risk-based. Second, details of that Program were organized in a separate section and were intended to be non-exclusive examples of possible ways to implement higher level requirements.[7]

    - In light of risk analysis and possible technological changes, Covered Entities should not be required to follow a formulaic approach. Also, if an entity already has a Cybersecurity Policy, the headings and order of the information may differ. By adding wording like "may include, but need not be limited to" before this list, entities may have more discretion while being in compliance with the standards.

- As an additional alternative, DFS could indicate that an entity would also be considered in compliance with this Section if its written policy uses a framework provided by one of the standard or government-sponsored organizations. For example, please consider the breadth offered by National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Federal Financial Institutions Examining Council (FFIEC) Cybersecurity Assessment Tool (CAT) and the International Organization for Standards (ISO).

[7] See Insurance Department Regulation 173 (and corresponding bank regulations).

CYBERSECURITY POLICY [BOARD REVIEW] - Section 500.03

(b) The cybersecurity policy shall be reviewed by the Covered Entity's board of directors or equivalent governing body and approved by a Senior Officer of the Covered Entity. If no such board of directors or equivalent governing body exists, the cybersecurity policy shall be reviewed and approved by a Senior Officer of the Covered Entity. Such review and approval shall occur as frequently as necessary to address the cybersecurity risks applicable to the Covered Entity, but no less frequently than annually.

Risk-Based:

- The level of detail for the Board to review should be risk-based. Each entity's cybersecurity policy may be structured with different levels of technological detail and complexity, perhaps varying based on any number of things (potentially including type of data, type of business, etc.).

- To keep the Board focused on meaningful aspects of the cybersecurity policy, the requirement would be more reasonable in scope if it referenced addressing "material" cyber security risks applicable to the entity (in the last sentence).

Flexible:

- To avoid going to the Board each time an entity needs to deviate from its cybersecurity policy, it may be helpful to allow explicitly for the Board to review and approve an appropriate authorized sign-off procedure for particular kinds of risks.

- To be efficient, Board review may be timely more or less frequently than annually. To accomplish this objective, it may be helpful to retain "as necessary" but to remove "but no less frequently than annually."

CHIEF INFORMATION SECURITY OFFICER - Section 500.04

(a) Chief Information Security Officer. Each Covered Entity shall designate a qualified individual to serve as the Covered Entity's Chief Information Security Officer ("CISO") responsible for overseeing and implementing the Covered Entity's cybersecurity program and enforcing its cybersecurity policy.
To the extent this requirement is met using third party service providers, 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 oversight of the third party service provider; and
(3) require the third party service provider to maintain a cybersecurity program that meets the requirements of this Part.

Flexible:

- To avoid duplicate administrative work without additional security benefit, because of the reference to "each Covered Entity," please clarify that nothing in the regulation precludes an entity within a group from using the cybersecurity program of an affiliated entity to the extent that those related entities are covered under the same cybersecurity program (for example, consider a parent and its subsidiary).

- To the extent DFS retains the third party service provider requirement in (3), consider changing the language to "take reasonable steps to select and retain" such vendors who are "capable of maintaining an appropriate cybersecurity program that substantially meets the requirements of this Part."

- There is concern that to be "qualified" such individual must be highly credentialed in this specific field. This may drive the cost to an unreasonable burden on smaller carriers and agents. To imbed a degree of flexibility in staffing, consider language like: "A CISO shall be deemed to be qualified by work experience in the information security field or by education or certification in technology, risk management or business."

- There is a concern that for smaller insurers (even those above the threshold) outsourcing the CISO function, the level of responsibility for third parties they would be required to maintain under this provision would be burdensome. This may have the unfortunate effect of chilling smaller companies from getting assistance from cybersecurity experts.

CHIEF INFORMATION SECURITY OFFICER - Section 500.04

(b) Report. The CISO of each Covered Entity shall develop a report, at least bi-annually, as described herein. Such report shall be timely presented to the 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. Such report shall be made available to the superintendent upon request. The report shall:
(1) assess the confidentiality, integrity and availability of the Covered Entity's Information Systems;
(2) detail exceptions to the Covered Entity's cybersecurity policies and procedures;
(3) identify cyber risks to the Covered Entity;
(4) assess the effectiveness of the Covered Entity's cybersecurity program;
(5) propose steps to remediate any inadequacies identified therein; and
(6) include a summary of all material Cybersecurity Events that affected the Covered Entity during the time period addressed by the report.

Risk-Based:

- To avoid a vulnerabilities road map within this Report, this Section could be framed as requiring a simple high-level summary that would (1) outline the overall status of the Covered Entity's cybersecurity program, and (2) reference material matters related to the development, implementation, and maintenance of a Covered Entity's cybersecurity policies and procedures (without going on to catalog in this Report those things listed in (3)-(6) of the Proposal).

- If retaining the list of specific items under (b), the provisions required under (2), (3) and (5) should include a materiality component.

- To avoid additional cybercriminal exposure by sharing a vulnerability roadmap, going forward DFS should support the Covered Entity retaining control and possession of the report.

- A strict "bi-annual" requirement for the report may be too frequent for some companies and may result in diverting the CISO's attention from addressing emerging and previously identified cyber risks.

Flexible:

- Rather than referencing making this report available to the Superintendent, please consider the existing thorough reviews DFS already has in place today.

- If a Covered Entity's cybersecurity policies and procedures document a risk-based exception procedure (setting forth things like eligible kinds of data with appropriate pre-determined internal authorizations), exceptions within the scope of those policy and procedures may not necessarily be the kinds of things that are intended to be reported under (b)(2). Wording to allow for such flexibility would be helpful.

PENETRATION TESTING AND VULNERABILITY ASSESSMENTS - Section 500.05
PENETRATION TESTING DEFINITION – Section 500.01(i)

(a) The cybersecurity program for each Covered Entity shall, at a minimum, include:
(1) penetration testing of the Covered Entity's Information Systems at least annually; and
(2) vulnerability assessment of the Covered Entity's Information Systems at least quarterly.

(i) ***Penetration Testing*** means a test methodology in which assessors attempt to circumvent or defeat the security features of an Information System.

Risk-Based:

- The Proposal frames these particular controls – penetration testing and vulnerability assessments – as mandatory for all Information Systems without accounting for the sensitivity of those systems or the nature of the information contained on them and without considering what other tools may be available. Narrowing the Information Systems definition to those that are sensitive would aid in directing attention and resources more effectively.

Flexible:

- By framing this Section with "as appropriate" wording in (a) (and removing "at a minimum"), DFS would empower entities to prioritize and to choose which tool(s) to use. Please note that not only may these tools change over time, but there may be other effective options available today.

- "Penetration testing" is one specific tool for assessing system security and mandating its use may be too rigid (and the Proposal's definition may not be broad enough to meet all of what may be considered penetration testing today). Further, because technology may become obsolete quickly, it may not be worthwhile to mandate one specific kind. Please reconsider whether one particular method for reviewing security weaknesses need be mandated. It might be helpful for DFS to indicate a more general principle (and potentially to include non-mandatory examples or references to some of the well regarded standard setting organizations or certifications).

- The cybersecurity policy should allow for the flexibility to schedule testing and assessments on a frequency it considers appropriate to the level of risk.

AUDIT TRAIL - Section 500.06

(a) The cybersecurity program for each Covered Entity shall, at a minimum, include implementing and maintaining audit trail systems that:

(1) track and maintain data that allows for the complete and accurate reconstruction of all financial transactions and accounting necessary to enable the Covered Entity to detect and respond to a Cybersecurity Event;

(2) track and maintain data logging of all privileged Authorized User access to critical systems;

(3) protect the integrity of data stored and maintained as part of any audit trail from alteration or tampering;

(4) protect the integrity of hardware from alteration or tampering, including by limiting electronic and physical access permissions to hardware and maintaining logs of physical access to hardware that allows for event reconstruction;

(5) log system events including, at a minimum, access and alterations made to the audit trail systems by the systems or by an Authorized User, and all system administrator functions performed on the systems; and

(6) maintain records produced as part of the audit trail for not fewer than six years.

Risk-Based:

- Going back to develop audit trails for all applications would be extremely time consuming and costly and may strain existing systems, with little to no improvement in protecting data. NAMIC asks DFS not to include this requirement.

- If DFS is going to retain this requirement, NAMIC asks that DFS greatly reduce the scope in several ways.

  First, limit the scope of the kinds of information to those systems that are higher-risk in nature given especially sensitive Information Systems. (Please see comments on definitions and note that otherwise "financial transaction" is undefined.)

  Second, the six-year minimum retention period poses a major concern. It would present a significant challenge to data storage, expanding from one institution creating several terabytes daily to petabytes of information being stored. Also, there may be differing time requirements where Payment Card Industry (PCI) is involved.

  Third, please consider only including audit trails as a design consideration going forward, rather than requiring entities to engage in a project to go through all existing systems and functions.

Given that the audit trail itself may not "protect" the hardware or the data, kindly consider softening the wording to the extent (3) and (4) are included in the regulation.

Flexible:

- The financial institution should have the flexibility under (6) to make a risk-based decision to maintain records as appropriate rather than for the across-the-board specified minimum timeframe.

- Further flexibility could be added throughout this provision by inserting "reasonable" in (a) to consider reasonable audit trail systems.

ACCESS PRIVILEGES - Section 500.07

As part of its cybersecurity program, each Covered Entity shall limit access privileges to Information Systems that provide access to Nonpublic Information solely to those individuals who require such access to such systems in order to perform their responsibilities and shall periodically review such access privileges.

Risk-Based:

- Given the scope of the definitions, the access privileges Section could require very detailed review of all systems (including significant numbers of legacy systems). Entities should be able to decide on access privileges based on the specific sensitivity of the information and the system as well as on the role of the individual. If DFS revises its definitions to sensitive Nonpublic Information and to sensitive Information Systems it will give the entity more flexibility to design access controls that reflect risk.

Flexible:

- Please consider inserting "reasonably" before "perform their responsibilities."

APPLICATION SECURITY - Section 500.08

(a) Each Covered Entity's cybersecurity program shall, at a minimum, include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, as well as procedures for assessing and testing the security of all externally developed applications utilized by the Covered Entity.
(b) All such procedures, guidelines and standards shall be reviewed, assessed and updated by the CISO of the Covered Entity at least annually.

Risk-Based:

- Requiring testing of all externally developed applications appears to go beyond a risk-based approach. Not all external applications pose the same threat or interact with Nonpublic Information. Please consider limiting (a) to those applications developed internally.

Flexible:

- Upon annual review required under (b), the CISO may decide that some procedures, guidelines and standards do not need to be "assessed and updated." Please consider removing those steps or inserting a qualifier like "as necessary."

RISK ASSESSMENT - Section 500.09

(a) At least annually, each Covered Entity shall conduct a risk assessment of the Covered Entity's Information Systems. Such risk assessment shall be carried out in accordance with written policies and procedures and shall be documented in writing.
(b) As part of such policies and procedures, each Covered Entity shall include, at a minimum:
(1) criteria for the evaluation and categorization of identified risks;
(2) criteria for the assessment of the confidentiality, integrity and availability of the Covered Entity's Information Systems, including the adequacy of existing controls in the context of identified risks; and
(3) requirements for documentation describing how identified risks will be mitigated or accepted based on the risk assessment, justifying such decisions in light of the risk assessment findings, and assigning accountability for the identified risks.

Risk-Based:

- To reflect a risk-based approach, NAMIC urges DFS to insert language to indicate that such cybersecurity program should be appropriate to the entity's size and complexity, the nature and scope of its activities and the sensitivity of the Nonpublic Information.

- By narrowing the focus of Information Systems to those that are sensitive in nature, entities could target their cybersecurity efforts more effectively.

Flexible:

- Compensating controls – those that substitute security controls in place of those required ones that are too difficult or impractical to implement – have a place for entities being able to mitigate risk in a workable way. It may be worthwhile to incorporate this concept into the risk assessment Section (and possibly into others as well). Kindly consider adding compensating controls to (b)(2) and removing the remainder of the provision in (3) after "risk assessment."

- As an additional alternative to the wording in the Proposal, DFS could indicate in a new (c) that provides that an entity would also be considered in compliance with this Section if its written policies and procedures use a framework provided by one of the standard or government sponsored organizations. For example, and brainstorming, please consider the breadth offered by National Institute of Standards and Technology (NIST) Cybersecurity Framework, the Federal Financial Institutions Examining Council (FFIEC) Cybersecurity Assessment Tool (CAT) and the International Organization for Standards (ISO).

- A risk assessment should be permitted on an enterprise-level rather than required separately for each Covered Entity.

CYBERSECURITY PERSONNEL AND INTELLIGENCE - Section 500.10

(a) Cybersecurity Personnel and Intelligence. In addition to the requirements set forth in 500.04(a), each Covered Entity shall:
(1) employ cybersecurity personnel sufficient to manage the Covered Entity's cybersecurity risks and to perform the core cybersecurity functions specified in section 500.02(b)(1)-(5) of this Part;
(2) provide for and require all cybersecurity personnel to attend regular cybersecurity update and training sessions; and
(3) require key cybersecurity personnel to take steps to stay abreast of changing cybersecurity threats and countermeasures.
(b) A Covered Entity may choose to utilize a qualified third party to assist in complying with the requirements set forth in this Part, subject to the requirements set forth in section 500.11 of this Part.

Risk-Based:

- The wording in (b) may not be necessary for all aspects of (a). For example, if a third party is only providing training and is not accessing sensitive systems or information, the risk of using such a third party may not warrant the level of scrutiny and contract provisions outlined Section 500.11 of the Proposal.

Flexible:

- With an understanding that situations may differ and may change quickly, consider expanding (a) to include "use reasonable efforts to" before the list of staffing requirements. For a smaller insurer or agent not qualifying for the exemption, dedicated staff meeting these requirements may be particularly burdensome.

- While financial institutions need to make independent management decisions on how and where to train their cybersecurity personnel (or how and where their qualified third party does so), it may also be helpful to reference standards and certain certifications as safe harbors (though not the sole means) for meeting the training requirement under (a)(2). For example, please consider referencing non-mandated examples of ways to comply with the training given the established training and certifications offered by organizations like SANS Institute.

- Cybersecurity staffing should be permitted on an enterprise-level rather than required separately for each Covered Entity.

THIRD PARTY INFORMATION SECURITY [WRITTEN] POLICY - Section 500.11(a)

(a) Third Party Information Security 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 parties doing business with the Covered Entity. Such policies and procedures shall address, at a minimum, the following areas: (1) the identification and risk assessment of third parties with access to such Information Systems or such Nonpublic Information; (2) minimum cybersecurity practices required to be met by such third parties 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 parties; and (4) periodic assessment, at least annually, of such third parties and the continued adequacy of their cybersecurity practices.

Risk-Based:

- Third parties are not all alike; they need to be differentiated based on the risk they pose to security. In looking at the level of risk, a Covered Entity may consider things like sensitivity and quantity of data accessed as well as the system the vendor may be accessing.
- Again, narrowing the scope to sensitive Nonpublic Information and Information Systems may help Covered Entities be able to prioritize the work that may need to get done as a result of the new requirement and to do so in a risk-based way.
- Because it is not feasible given the volume of third party relationships, please strike "at least annually" in (a)(4) so that a Covered Entity has the flexibility to engage in their assessments of third parties in a way that focuses most frequently on those that are the greatest concern.
- The last sentence before the list of items to be included in the policy could use wording like "reflect a risk management process in considering" in place of "address, at a minimum."

Flexible:

- Given the large volume of contracts and vendors and the level of review outlined in the Proposal, please consider the possible value in adding optional safe harbors that indicate:
    - Covered Entities may, but need not, rely upon a third party being a DFS Covered Entity as evidence that such third party will meet the DFS required standards.
    - Covered Entities may accept and rely upon a third party's independent reports or certifications reviewing their operational/data security controls.
- Because the word "ensure" may imply absolute certainty, kindly consider "protect" in its place.
- To increase judgment in light of the risk, consider inserting "appropriate" in several places (in place of "minimum" in (a)(2), in place of "due diligence processes used to evaluate the adequacy of" in (a)(3) and in place of "at least annually" in (a)(4)). Also, consider including "contractual assurance from such third parties" at the beginning of (a)(3).
- To inject a reasonableness approach, the Proposal may be more manageable if changed to insert "to use reasonable efforts" after "designed" in (a) and to replace "required" in (a)(2) with "as may be reasonably agreed to by the parties based on the Covered Entity's risk assessment."
- Given that there may be compensating controls or ways to mitigate challenges posed by third parties, kindly consider whether the last sentence in (a) before the list indicates that the Covered Entity shall "consider" the following in developing such Third Party Information Security Policy.

THIRD PARTY INFORMATION SECURITY POLICY [CONTRACTS] - Section 500.11(b)

(b) Such policies and procedures shall include establishing preferred provisions to be included in contracts with third party service providers, including provisions addressing, to the extent applicable: (1) the use of Multi-Factor Authentication as set forth in Section 500.12 to limit access to sensitive systems and Nonpublic Information; (2) the use of encryption to protect Nonpublic Information in transit and at rest; (3) prompt notice to be provided to the Covered Entity in the event of a Cybersecurity Event affecting the third party service provider; (4) identity protection services to be provided for any customers materially impacted by a Cybersecurity Event that results from the third party service provider's negligence or willful misconduct; (5) representations and warranties from the third party service provider that the service or product provided to the Covered Entity is free of viruses, trap doors, time bombs and other mechanisms that would impair the security of the Covered Entity's Information Systems or Nonpublic Information; and (6) the right of the Covered Entity or its agents to perform cybersecurity audits of the third party service provider.

Risk-Based:

- Applying identical standards to every third party may distract from good risk management practices which evaluate risks and prioritize accordingly. Because a single contract management and drafting approach may not fit in all instances, please consider inserting wording like "technically feasible and appropriate" in place of "applicable."

- The trigger for third party notice to the Covered Entity under (b)(3) and for identity theft protection services under (b)(4) should be a breach or incident (or a "material" Cybersecurity Event) rather than the broad Cybersecurity Event defined in the proposal. The event may not be material (unless determined to be an incident or breach) and notice of an event would inundate all parties.

- As discussed for Covered Entities, encryption at rest is likely an issue for third parties as well (and the greater risk is generally thought to be data in transit). If changes are made to that section and if DFS must include encryption going forward for third parties, perhaps cross reference Section 500.15 here. Similarly, if changes are made to the authentication section and if DFS must include authentication provisions in Covered Entity contracts with third parties it may be cleaner to cross reference that Section 500.12.

Flexible:

- Third parties may not be willing to accept contract terms consistent with the Proposal. For example, the third party may provide only a limited liability (for example up to the amount paid for the product or service) rather than providing a larger warranty or accepting a bigger responsibility for liability. Not only should this be a business negotiation between commercial entities, the requirement in (b)(5) could be extremely disruptive to existing contracts and consequently to the corresponding services provided (and it may be difficult to find and finalize replacement vendors given the volume of third parties and the effective date. Also, the language in (b) could be revised to indicate that the preferred provisions are to be "available" for contracts with third party service providers (rather than to be mandated to be "included" in them).

- Audits may not be appropriate or able to be negotiated in all situations. Consider changing the approach in (6) to allow the Covered Entity to be permitted to use reasonable due diligence to assess (not necessarily "audit") the cybersecurity practices of the third party service provider.

- Given the changing nature of technology, some entities may elect to attach an IT exhibit (which may be modified periodically as technology changes and security advances) to their contracts. Things like multi-factor authentication and encryption that address the technological how-to may be in such an exhibit. Perhaps indicate in (b) that it could be included in a contract "or in an Exhibit thereto."

- Third party contract handling may be another area where it would be beneficial to reference an option of complying by following particular federal government guidance or standards setting organization approaches.

AUTHENTICATION / MULTI-FACTOR AUTHENTICATION - Section 500.12

(a) Multi-Factor Authentication. Each Covered Entity shall: (1) require Multi-Factor Authentication for any individual accessing the Covered Entity's internal systems or data from an external network;[8] (2) require Multi-Factor Authentication for privileged access to database servers that allow access to Nonpublic Information;[9] (3) require Risk-Based Authentication in order to access web applications that capture, display or interface with Nonpublic Information; and (4) support Multi-Factor Authentication for any individual accessing web applications that capture, display or interface with Nonpublic Information.

Risk-Based:

- Whether heightened authentication methods may be necessary should depend on the risk presented (type and extent of access, information, servers, etc.). Please consider revising (a) to underscore that requirements should be undertaken as appropriate to a Covered Entity's size and complexity, the nature and scope of its activities and the amount and sensitivity of the Nonpublic Information. Without financial account or other sensitive information, which may present a higher risk of consumer harm in the hands of a criminal, consider whether the Covered Entity should be required to provide additional new security at great expense (especially on older legacy systems).

- If requiring this particular form of authentication, kindly consider narrowing the scope to only apply to employees accessing sensitive internal systems or networks remotely through a virtual private network (VPN) and defining "web-based applications" so that applications made available to employees on the entity's network using web protocols (http or https) are not included. This may allow for a more risk-based approach to monitor and guard the most sensitive data, while still allowing alternative controls.

- Because technology changes over time and alternate effective (and potentially preferred to multifactor authentication) authentication controls may already exist and because risks differ, please consider framing this provision by requiring the Covered Entity to have adequate processes in place to authenticate credentials of or to confirm the identity of the authorized user gaining access to Nonpublic Information.

- Some entities may opt to allow simpler authentication for access to more basic customer information and to increase authentication activities (layered controls) as a customer engages in additional types of activity which seek to access more sensitive information. This risk-based approach may allow for a less frustrating and more customer friendly experience for some users, while still protecting the most sensitive information.

Flexible:

- Multifactor authentication is a way to limit access to authorized users. By mandating one specific method for managing access, the Proposal may deter entities from using other methods of authentication that may be appropriate today (including reviewing an IP address) as well as those that may be effective in the future. Additional flexibility is warranted. Noting relatively low take-up rates on some authentication types, it may be helpful for (b)(4) customer access to limit the scope to those web applications that contain sensitive nonpublic information and to allow the Covered Entity to find an appropriate authentication method including but not limited to multifactor authentication.

- There may be some instances when it is not technically feasible to use multi-factor authentication.

- Framing this section more generally as adequate processes to authenticate credentials, multifactor authentication could be included as a non-exclusive example of an available approach.

- The meaning of "privileged access" in (a)(2) may be unclear. Consider when the privilege is view-only access (without the ability to move or spend money) to limited information. Please allow common sense risk-based flexibility.

[8] The connection access point for an individual internally may be through an internal network (rather than systems or data) from an external network.

[9] The concern may be with privileged access to systems or servers (rather than database servers) that allow direct access to certain Nonpublic Information.

LIMITATIONS ON DATA RETENTION[10] - Section 500.13

As part of its cybersecurity program,[11] each Covered Entity shall include policies and procedures for the timely destruction of any Nonpublic Information identified in 500.01(g)(2)-(4) that is no longer necessary for the provision of the products or services for which such information was provided to the Covered Entity, except where such information is otherwise required to be retained by law or regulation.

Risk-Based:

- Consider referencing sensitive Nonpublic Personal Information which presents a higher risk.

Flexible:

- NAMIC strongly encourages DFS to amend the Proposal to indicate that disposal trigger under this Section is when the applicable information would no longer be "retained" by the Covered Entity (and removing the remainder of the wording beginning from "necessary"). This additional wording generates many questions and concerns.

- New York has a general business law addressing disposal of records containing personal identifying information.[12] That law contains a few concepts that may be useful to consider here. For example, "destruction" is not the only means of disposal. It may also be acceptable to modify the record to make the information unreadable or to follow another commonly accepted industry practice that an entity reasonably believes will ensure there would be no unauthorized access to the information. Consider changing the wording to "secure disposal" in place of "timely destruction."

[10] It appears Section 500.13 is geared primarily at addressing disposal of records rather than at retaining them. Consider revising the reference to "retention" in the section title.

[11] Because cybersecurity program is not a defined term, consider whether to cross reference Section 500.02.

[12] See New York General Business Law Section 399-h.

TRAINING AND MONITORING - Section 500.14

(a) As part of its cybersecurity program, each Covered Entity shall:
(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) provide for and require all personnel to attend regular cybersecurity awareness training sessions that are updated to reflect risks identified by the Covered Entity in its annual assessment of risks.

Risk-Based:

- Consider referencing sensitive Nonpublic Information which presents a higher risk.
- A targeted risk-based approach to training in (a)(2) may involve: (i) using reasonable efforts; and (2) requiring training of the personnel the CISO has identified and/or of the personnel with access to Nonpublic Information.

Flexible:

- To allow for possible unanticipated situations (especially for subsequent training), consider inserting "use reasonable efforts to" at the beginning of (a)(2).
- Consider providing that the Covered Entity (or its affiliate) has flexibility in how it delivers the training sessions (in order to allow for webinars).

ENCRYPTION OF NONPUBLIC INFORMATION - Section 500.15

(a) As part of its cybersecurity program, each Covered Entity shall encrypt all Nonpublic Information held or transmitted by the Covered Entity both in transit and at rest.
(b) To the extent encryption of Nonpublic Information in transit is currently infeasible, Covered Entities may instead secure such Nonpublic Information using appropriate alternative compensating controls reviewed and approved by the Covered Entity's CISO. Such compensating controls shall not be used in lieu of meeting the requirements of subsection 500.15(a) after one year from the date this regulation becomes effective.
(c) To the extent encryption of Nonpublic Information at rest is currently infeasible, Covered Entities may instead secure such Nonpublic Information using appropriate alternative compensating controls reviewed and approved by the Covered Entity's CISO. Such compensating controls shall not be used in lieu of meeting the requirements of subsection 500.15(a) after five years from the date this regulation becomes effective.

Risk-Based:

- Encryption of nonpublic information for data at rest would be cost-prohibitive for many entities (especially those with old legacy systems) and may not be the most appropriate control to prevent threats to at-rest data. Therefore, NAMIC strongly and respectfully urges DFS not to include a requirement for at-rest encryption in the regulation.

- For encryption in transit, NAMIC urges DFS to specify that the requirement would be limited to where the risk is the greatest:

    - To sensitive Nonpublic Information.

    - Being moved externally over a public network (rather than through an internal network).

Flexible:

- By sunsetting the compensating controls alternative (and linking compensating controls to situations where encryption is infeasible), DFS appears to imply that encryption is an infallible solution today and that it will remain the best way to protect data in the future. NAMIC encourages DFS to retain those control options without limitation.

- As discussed in NAMIC's comments to the Introduction and elsewhere in this letter, it would be highly beneficial to structure the regulation around high-level concepts and then indicating non-exclusive examples of ways to comply. This would help to avoid dependence on a single solution as well as obsolescence. It may also help to permit Covered Entities to be able to use valid controls and processes from certain standards organization. Encryption may be a useful example of where this approach may work well.

INCIDENT RESPONSE PLAN - Section 500.16

(a) As part of its cybersecurity program, each Covered Entity shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event 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.

(b) Such incident response plan shall, at a minimum, address the following areas:

(1) the internal processes for responding to a Cybersecurity Event;
(2) the goals of the incident response plan;
(3) the definition of clear roles, responsibilities and levels of decision-making authority;
(4) external and internal communications and information sharing;
(5) remediation of any identified weaknesses in Information Systems and associated controls;
(6) documentation and reporting regarding Cybersecurity Events and related incident response activities; and
(7) the evaluation and revision of the incident response plan following a Cybersecurity Event.

Risk-Based:

- To reflect a more risk-based approach wording could be revised, perhaps by inserting reasonableness and materiality (consider "reasonably designed" in (a)).

- Consider an incident response plan triggered off a breach (as compared to a Cybersecurity Event Response Plan). Kindly see comments in this letter regarding concerns relating to a definition that includes unsuccessful attempts (as included in the Proposal's definition of a Cybersecurity Event) as well as a broad definition of Nonpublic Information (as compared to financial institutions' current understanding of nonpublic information under existing law).

- Consider amending this Section to allow the Covered Entity to consider whether accessed information was able to be read (for example whether it was encrypted) as well as the scope and nature of information. Additionally, it would seem appropriate for an Incident Response Plan to consult applicable laws.

Flexible:

- For administrative ease and understanding that the substance of incident response may be in place already, an entity should be permitted to house its incident response plan as a stand-alone program or within its cybersecurity program or other program(s)/plan(s).

- To avoid duplicate administrative work without additional security benefit, please clarify that nothing in the regulation precludes an entity within a group from using the cybersecurity program of an affiliated entity to the extent that those related entities are covered under the same cybersecurity program (for example, consider a parent and its subsidiary).

- Consider whether there are ways to allow explicitly for using certain standards or guidelines as an optional safe harbor. Perhaps it would be helpful for DFS to further gather information about such standards.[13]

[13] One organization mentioned was the International Organization for Standardization (ISO).

NOTICES TO SUPERINTENDENT & "CYBERSECURITY EVENT" - Section 500.17

(a) Notice of Cybersecurity Event. Each Covered Entity shall notify the superintendent of any Cybersecurity Event that has a reasonable likelihood of materially affecting the normal operation of the Covered Entity or that affects Nonpublic Information. The Covered Entity must notify the superintendent as promptly as possible but in no event later than 72 hours after becoming aware of such a Cybersecurity Event. Such Cybersecurity Events include, but are not limited to:
(1) any Cybersecurity Event of which notice is provided to any government or self-regulatory agency;
(2) any Cybersecurity Event involving the actual or potential unauthorized tampering with, or access to or use of, Nonpublic Information.

Risk-Based – Notice to Superintendent:

- To provide DFS with meaningful information and to avoid significant numbers of reports daily that will not reduce cyber threats, NAMIC encourages DFS to amend the "Cybersecurity Event" definition or terminology in order to focus on material incidents.

- Replacing this Subsection of the Proposal with a requirement that if a DFS-regulated entity sends a breach notice as required by New York General Business Law Section 899-aa(8)(a) it must notify the Superintendent, seems to be a clean approach given that the New York breach law imbeds a sensible risk of harm trigger because its definition of applicable "personal information" carves out instances where the unauthorized person is unlikely to access information because the information is unreadable because it is encrypted (and without an encryption key). NAMIC advocates for this approach. This approach would also avoid confusion of conflicting definitions, triggers and requirements. Kindly compare carefully the definitions and triggers between "breach of the security of the system" contained in the existing law and "cybersecurity event" under the Proposal. New York's breach requirements[14] outline the trigger for providing notice: risk of harm to customer data is an unauthorized "acquisition of and use of Nonpublic Information" rather than "tampering with" information.

- This Section highlights concerns with the scope of the Cybersecurity Event definition (and its omission of a material risk of harm standard) and of the Nonpublic Information definition (which is so broad). As the Proposal stands, the Superintendent would be inundated with notices for Cybersecurity Events of little or no consequence and Covered Entities would be obligated to spend time and expense generating such useless notices. Indeed, a single person incorrectly entering a password and therefore presumed to be an unsuccessful attempt to gain unauthorized access would trigger this requirement. Changing the definitions to limit requirements to successful attacks compromising important personally identifiable customer data may have the downstream effect of making the substantive provisions more workable.

- The Superintendent notice requirement in (a) should be limited to sensitive Nonpublic Information, where the risk is the greatest.

[14] See New York General Business Law Sec. 899-aa. Many states have breach notice laws based in whole or in part on the American Legislative Exchange Council (ALEC) model, "The Breach of Personal Information Notification Act."

Flexible – Notice to Superintendent:

- Respectfully, the company confidential component of the Nonpublic Information definition should be removed because of its impact on Sections like this one. In the absence of a breach or cyber event, DFS has other tools available for understanding insurers' cybersecurity and risk. As noted by DFS in its Report on Cyber Security in the Insurance Sector (February 2015), which followed a survey of insurers as well as meetings with them, DFS has the authority to review cyber protections and programs as part of statutorily required enterprise risk management (ERM) reports.[15] Additionally, DFS IT examiners may review cyber security through their cyber security examination. Further, a compromise of confidential trade secret information may be addressed in an entity's business continuity plan.

- A Cybersecurity Event (or incident) that did not impact a New York resident should not require a notice to the New York regulator.

Risk-Based – 72 Hours:

- NAMIC asks that no time frame be include in the regulation. If tied to the Section 899-aa(8)(a) notice under the breach law this would not be necessary.

- When a Cybersecurity Event (using the Proposal's broad definition) occurs, an entity would then research the incident to learn about the extent of harm (nature of any technological vulnerability, whether any information was compromised and if so, the nature of that information). Despite best efforts, that information about materiality may not be available instantly. If DFS must proceed with a time limitation, it should run from the time that a determination has been made that a breach has occurred. Before such determination has been made, the entity may not be able to provide the Superintendent with useful information regarding the nature and extent of the event.

Flexible – 72 Hours:

- Working from the existing law for purposes of the timing of the notice would be helpful as well. That law provides for a delay "if a law enforcement agency determines that such notification impedes a criminal investigation."[16] Following the same approach (either by reference or directly) would take account of this legislative deference to law enforcement in cybercrime. This is even more important given that confidentiality of reporting is not provided for under the Proposal.

[15] See Insurance Regulation 203, 11 N.Y.C.R.R. Part 82.
[16] See New York General Business Law Section 899-aa(4).

NOTICES TO SUPERINTENDENT & "CYBERSECURITY EVENT" - Section 500.17

(b) Annually each Covered Entity shall submit to the superintendent a written statement by January 15, in such form set forth as Appendix A, certifying that the Covered Entity is in compliance with the requirements set forth in this Part. Each Covered Entity shall maintain for examination by the Department all records, schedules and data supporting this certificate for a period of five years.
(1) To the extent a Covered Entity has identified areas, systems, or processes that require 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.
(2) To the extent that a Covered Entity has identified any material risk of imminent harm relating to its cybersecurity program the Covered Entity shall notify the superintendent within 72 hours and include such items in its annual report filed pursuant to this section.

Risk-Based:

- NAMIC respectfully asks that DFS remove the 72 hour notice requirement, (b)(2) for the reasons indicated in comments on Subsection 500.17(a) above. Again, DFS has the authority to review cyber protections and programs as part of statutorily required enterprise risk management (ERM) reports[17] and DFS IT examiners may review cyber security through their cyber security examination.

- To better reflect risk, it would be helpful for the scope of (b)(1) to be limited to sensitive Information Systems.

- As with the CISO report under Section 500.04, to avoid additional cybercriminal exposure by sharing a vulnerability roadmap that indicates planned and ongoing remedial efforts, going forward DFS should support the Covered Entity retaining control and possession of the report.

Flexible:

- To the extent DFS retains a time requirement, NAMIC urges that that the time run from the time that a determination has been made that a breach has occurred and that it may be tolled if requested by law enforcement.

[17] See Insurance Regulation 203, 11 N.Y.C.R.R. Part 82.

LIMITED EXEMPTION - Section 500.18

(a) Limited Exemption. Each Covered Entity with: (1) fewer than 1000 customers in each of the last three calendar years, and (2) less than $5,000,000 in gross annual revenue in each of the last three fiscal years, and (3) less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all Affiliates, shall be exempt from the requirements of this Part other than the requirements set forth in this section, Sections 500.02, 500.03, 500.07, 500.09, 500.11, 500.13, 500.17, 500.19, 500.20 and 500.21.
(b) In the event that a Covered Entity, as of its most recent fiscal year end, ceases to qualify for the limited exemption as set forth in subsection 500.18(a), such Covered Entity shall have 180 days from such fiscal year end to comply with all requirements of this Part.

Flexible:

While entities of all sizes have expressed their concerns with the scope of and mandates in the Proposal, it should be expected to impact smaller entities hardest. NAMIC strongly encourages DFS to:

- Replace “and” with “or” between the requirements in (a);
- Increase the number of customers, the gross annual revenue dollar amount and the year-end total asset dollar amount thresholds;
- Clarify that the thresholds relate to New York specific customers and dollars (rather than including out-of-state business);
- Clarify that the total assets in (a)(3) relate to financial services affiliates licensed by DFS; and
- Expand the list of Sections to which exempt entities would not be subject to include 500.06 (audit trail) (and depending on revisions to the Proposal, perhaps additional sections as well).

EFFECTIVE DATE & TRANSITION PERIOD - Section 500.20 / Section 500.21

Before turning to the proposed effective date provision, NAMIC respectfully suggest that DFS consider breaking this complex topic into multiple stand-alone regulations or to a regulation to be supplemented on a periodic basis as implementation an execution by both the NY DFS and by the industry provides experience to make the standards both effective and efficient. The subject matter lends itself well to staggered implementation and using the time between those implementation dates to consider and address carefully each of the topics would serve the administration, customers and the business community well.

Section 500.20 Effective Date. This part will be effective January 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 commencing January 15, 2018.

Section 500.21 Transitional Period. Covered Entities shall have 180 days from the effective date of this regulation to comply with the requirements set forth in this Part, except as otherwise specified.

- For a general transition period, given the scope of the Proposal as well as project (budget, staffing, systems) planning, NAMIC urges that DFS provide a 24-month period.

- For the Third Party Information Security Policy under Section 500.11, NAMIC asks that that period be longer, given the extent of the contract project and the scope of the definitions. There is precedent for including grandfathering provision for existing third party contract. This was done in New York's implementing regulations following Gramm-Leach-Bliley.[18]

- For some provisions, NAMIC asks if DFS would consider drafting certain requirements to apply only on a prospective basis. Please consider the significant cost and time-consuming exercise to perform an application by application to review and/or build certain controls for older legacy systems that may not pose material risk. For example, please consider Multi-Factor Authentication under Section 500.12.

Finally, NAMIC members are extremely interested in working with the DFS on revisions to the Proposal. On their behalf, NAMIC respectfully requests that DFS to allow a full opportunity for insurers to review and comment meaningfully on any revisions with adequate time before the Effective Date.

[18] See Section 420.24(c) of Regulation 169 addressing "Privacy of Consumer Financial and Health Information."

Certification of Compliance – APPENDIX A

Certification of Compliance with New York State Department of Financial Services Cybersecurity Regulations
The Board of Directors or a Senior Officer(s) of the Covered Entity certifies:
(1) The Board of Directors (or name of Senior Officer(s)) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals or entities as necessary;
(2) To the best of the (Board of Directors) or (name of Senior Officer(s)) knowledge, the Cybersecurity Program of (name of Covered Entity as of____(date of the Board Resolution or Senior Officer(s) Compliance Finding) for the year ended (year for which Board Resolution or Compliance Finding is provided) complies with Part ___.
(3) Signed by the Chairperson of the Board of Directors or Senior Officer(s)

Risk-Based:

- While the Certificate seems like a basic template to aid governance on cybersecurity, it may generate many layers of sign-offs and lasting paperwork while not targeting the essence of what DFS appears to be charging entities to do. NAMIC recommends removing this requirement as a certification, especially in the near term.

- If DFS moves forward with the certification, NAMIC urges DFS to:

  - Amend (2) to use an approach consistent with the requirements of the Proposal and certify that the programs, policies and procedures are in place rather than certifying to compliance. "Compliance" has legal and fiduciary implications and may be difficult to certify if DFS is looking to measure a standard of effectiveness of a Cybersecurity Program.

  - Clarify (1) to provide additional guidance to qualify the level and volume of "documents, reports, certifications and opinions" from "officers, employees, representatives, outside vendors and other individuals or entities as necessary."

Flexible:

- If DFS moves forward with the certification, NAMIC asks that DFS consider that it does not appear to allow for varying levels of compliance (where perhaps some of the new controls in the Proposal are still being implemented or where a new risk has been identified and addressed).

- If applicable to more than one entity in a group, NAMIC asks that DFS allow for a consolidated Certification.

CONCLUSION

A flexible risk-based approach, in which cyber security programs are tailored to a measurement of the relevant risks), is essential to a long-lasting cybersecurity regulation. An overly prescriptive regulation cannot keep pace with technological advances. Consumers and financial institutions are better served when limited resources are prioritized to protect nonpublic customer information effectively. In these comments, NAMIC notes the importance of integrating a risk-based approach into the provisions and injecting greater flexibility.

NAMIC strongly urges DFS to reconcile the Proposal with existing New York laws, regulations and regulatory practices in other areas such as financial oversight, as well as federal guidance, by considering the risk-based standards that encourage and bolster financial institution cybersecurity efforts. Overlapping or conflicting laws (within New York and possibly across the country) may strain and slow efforts to protect data, especially where staff (technology and others) and internal policies and procedures may be the same regardless of state lines.

To the extent DFS moves ahead with requests for reports and notices or DFS expects to review entity cybersecurity-related information, NAMIC asks that a strong and effective confidentiality (or exemption from disclosure) protection be included.

Again, NAMIC asks for industry to have an opportunity to remain involved as DFS continues to consider this issue and to see revisions to the Proposal before it is published. Insurers invest heavily in cybersecurity; regulatory wording may have significant impact on operations and expenses.

NAMIC appreciates your consideration of these comments.

Respectfully,

Cate Paolino
Director – State Affairs, Northeast Region
National Association of Mutual Insurance Companies (NAMIC)

Cc: Maria T. Vullo, Superintendent DFS
Scott Fischer, Executive Deputy Superintendent for Insurance
Stephen Doody, DFS Deputy Superintendent for Property & Casualty
Alexander Sand, DFS Counsel, Capital Markets Division
Joan Riddell, Deputy Chief Insurance Examiner
Katie Neer, Governor Cuomo's Office
Tanisha Edwards, Assistant Counsel to Governor Cuomo