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

January 27, 2017

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 500

Dear Deputy Superintendent Lentchner:

On behalf of National Association of Mutual Insurance Companies (NAMIC)[1] members, I am writing to express appreciation to the New York Department of Financial Services (DFS) for the opportunity for insurers to meet with DFS regarding cybersecurity processes and opportunities and for DFS' willingness to consider presented concerns when developing the more risk-based approach reflected in the revised proposed regulation on Cybersecurity Requirements for Financial Services Companies ("Revised Proposal"). I am also writing to ask DFS to consider a few additional items before implementation.

First, some suggest that a few technical changes to the Revised Proposal would be helpful in clarifying the intent and scope of the requirements.

Under Section 500.01(g), the definition of ***Nonpublic Information*** should be limited explicitly to New York residents. In addition, NAMIC asks that "in any form or medium" wording in (3) be removed because the focus of the Revised Proposal is on electronic information vulnerable to cybersecurity concerns.

Under Section 500.01(i), the definition of ***Penetration Testing*** refers to a "database." From what I understand, such testing would usually be accomplished at the front end or "network" level than on the back end looking at the data itself.

Under Section 500.06, which addresses ***audit trail***, reference is made in (a)(1) to "material financial transactions." It may be helpful to regulated insurance entities to confirm that the intent is to address the material transactions supporting the institution, similar to what is considered under the Sarbanes-Oxley Act. Also under this section, while members appreciate the five years in place of six, they remain concerned about the length of the retention period.

Under Section 500.14, which addresses ***training and monitoring***, reference is made in (a)(2) to "all personnel." Referring to "employees" rather than "personnel" would remove doubt about the scope of the term. If there are obligations relating to outside contractors, those could be further articulated in Section 500.11.

[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.

Under Section 500.16, which outlines the ***incident response plan*** requirements, reference is made in (b)(5) to identification of requirements for remediation. Remediation of "any" weakness appears overbroad. Kindly see the following suggestion to target efforts on incident cause and future prevention: "(5) process for post-incident after action reviews to identify the cause of the incident and the steps necessary to prevent similar incidents in the future ~~identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls~~."

Under Section 500.18, which contains the ***confidentiality*** provision, given the nature of the information, covered entities should be allowed to request an exemption from disclosures for sensitive business information (trade secrets, competitive information, etc.). For example, kindly see the following suggestion: "Information provided to the Superintendent by a Covered Entity pursuant to this Part is subject to exemptions from disclosure under any relevant provision of the Banking Law, Insurance Law, Financial Services Law, Public Officers Law or any other applicable state or federal law including, without limitation, requesting that the Superintendent except such information from disclosure pursuant to the Public Officers Law section 89(5)(a)(1)."

Under Section 500.19, which outlines ***exemptions***, in (a)(1) please consider limiting the types of independent contractors to those that perform a core business function of the covered entity and that are not working on a temporary basis.

Also, some express that the ***extraterritorial application*** of the Revised Proposal is unclear. For example, there are questions as to whether DFS anticipates separate standards for a New York operation (the identifying of which may be complicated) or whether an existing or enhanced group approach could be used to meet the DFS requirements.

Second, to establish a formal dialogue and to recognize the speed at which technology changes, NAMIC asks NY DFS to institute a ***regular meeting***, at least twice a year, between an industry working group and DFS.

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