November 10, 2016

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

RE: Comments on proposed 23 NYCRR 500 - Cybersecurity Requirements for Financial Services Companies

Dear Ms. Lentchner:

We are writing on behalf of the Information Security Advisory Group, a group of company and agent representatives from the Independent Insurance Agents and Brokers of New York (IIABNY), New York Insurance Association (NYIA) and Professional Insurance Agents of New York (PIANY). Our advisory group was established to discuss how the insurance industry can protect retained policyholder data and enhance information security. One major outcome of our work is Guiding Principles to Advance Information Security in New York.

These principles are intended to serve as a broad road map for agents and companies. They were developed through a roundtable discussion of representatives from the agent and carrier communities with the discussion facilitated by the Center for Internet Security. The goal of the principles is to create a strong working relationship within the insurance industry to ensure agencies, companies and policyholders are better protected.

Each of our respective associations will be submitting separate substantive comments, but we wanted to communicate with you on behalf of the Information Security Advisory Group with our unique perspective on this topic and share our insights.

The insurance industry takes the responsibility of protecting policyholders very seriously. It is the very nature of our business. We provide financial security to individuals and businesses and by extension are committed to protecting policyholder data. We strongly believe in the need for every entity that holds any truly nonpublic information of its customers to have a cyber security and information security program and policy, but the program and policy must be risk-based and flexible so it can be tailored to the size, complexity and security needs of an entity.

The two proven essential elements of information security are working collaboratively and sharing information. The public and private sectors for years have worked with cyber experts and law enforcement to more effectively thwart attacks. Since the threats that exist are carried out by criminals, it is critically important that entities rely on collective knowledge and not operate in a vacuum. New challenges continually arise because information security is an ever evolving issue. A serious threat today could virtually disappear or morph significantly in a matter of months, only to be replaced by something completely different that requires a different approach. One key fact that has emerged is that threats are not specific to cyber. We view

iiabny Independent Insurance Agents & Brokers of New York, Inc. Trusted Choice

NYIA New York Insurance Association, Inc.

PIA Professional Insurance Agents

this issue as information security because breaches are being perpetrated through means that are not exclusively technological in nature, including stealing information by breaking into a building and obtaining sensitive information over the phone from an unsuspecting individual.

We urge DFS to take an approach that is risk-based and encourages and enables companies to assess their own risk and determine where vulnerabilities exist. Security is something that needs to be looked at on a company by company and agency by agency basis. All regulatory efforts should focus on what activities will make a company or agency better protected. Certain aspects of the proposed regulation are more strictly compliance-based such as the audit trail requirements and the notice to DFS. The notice is of particular concern because it deviates so significantly from federal and state law.

We will only touch on a few specific matters and leave further elaboration and potential alternatives to the comments provided by our respective associations.

There are numerous concerns with respect to section 500.11, Third Party Information Security Policy. Since there is no express definition of a "third party" in the regulation, it is unclear whether "third parties doing business with the covered entity" includes a covered entity doing business with another covered entity. For example, are insurance companies and insurance agencies both considered third parties because they do business with each other (i.e., a covered entity)? We believe that a covered entity would not be a third party based on the proposed regulation's language governing covered entities, but it would be extremely helpful to clearly define a third party as a non-covered entity that does business with a covered entity.

Also related to the third party provision, as a practical matter it will be extremely difficult to meet the compliance standards set out in this proposed regulation within 180 days after January 1, 2017. A related serious issue is the requirement to obtain representations and warranties from third party service providers that would ensure the service or product delivered to the insurance company or agency is free of viruses, trap doors, time bombs and other mechanisms capable of impairing the security of the insurance company's or agency's information systems or nonpublic information. Entities of all sizes are concerned about their ability to amend vendor agreements to include these assurances. In particular, smaller insurance companies and agencies will likely not be capable of obtaining these contractual guarantees due to their lack of bargaining power. It is important to consider the potential ramifications the stringent requirements and timeframe could have as well as the unintended consequence of limiting a company's ability to utilize the services of small businesses.

We also need to make certain that any information provided to DFS is provided and maintained in an extremely secure environment. In addition, confidentiality protection is absolutely essential. Any information that a covered entity provides to DFS should not be shared or accessible to outside inquiries via Freedom of Information Law or other means.

One alternative to the proposed regulation that would incorporate a flexible, risk-based approach is to reemphasize the applicability of Insurance Regulation 173 to all insurance law licensees (this may require exempting such licensees from the proposed regulation). Regulation 173, contained in 11 New York Code of Rules & Regulations (NYCRR) Part 421 (standards for safeguarding customer information), sets forth broad requirements, allowing insurers and agencies to tailor their cyber security programs in a flexible, risk-based

manner. More specifically, 11 NYCRR section 421.2 (information security program) requires each licensee to "implement a comprehensive written information security program that includes administrative, technical and physical safeguards for the protection of customer information." Most importantly, this section goes on to mandate that these safeguards "shall be appropriate to the size and complexity of the licensee and the nature and scope of its activities."

We ask that DFS continue to talk with the insurance industry and that we work together on this complex issue as no entity is immune from cyber risk. There is a great deal of expertise within the industry, and IIABNY, NYIA and PIA urge DFS to collaborate with property and casualty insurance companies and agencies as we all share the same concerns.

We appreciate the opportunity to provide our input on this very important subject, a subject that the insurance industry has been working diligently on for many years and remains focused on since risks are always evolving. We look forward to continued dialogue as the industry takes all reasonable steps to protect our policyholders.

Sincerely,

The Information Security Advisory Group

Peter Balisteri, Chief Information Officer, Merchants Insurance Group
Margaret Black, Vice President, Operations, Allan M. Block Agency Inc.
Steven Coffey, President and CEO, Broome Co-operative Insurance Company
Tim Dean, President, Marshall & Sterling, Inc.
Stuart Durland, AINS, AAI, Vice President of Operations, Seely & Durland Inc.
Andrew Forstenzer, General Counsel, Preferred Mutual Insurance Company
Edgar Higgins, Jr., CPCU, Vice President, Thousand Islands Agency
Fred Holender, Director of Administration, Lawley Service, Inc.
Lauren Pachman, Counsel & Director of Regulatory Affairs,
National Association of Professional Insurance Agents
Jeffrey Rice, President and CEO, Wayne Cooperative Insurance Company
George Robertson, Executive Board Member, ACT Security Issues Working Group
Keith Savino, Managing Partner, Warwick Resource Group, LLC
Richard Shlotzhauer, Senior Vice President Information Technology, Utica First Insurance Company
Karen Skarupski, Senior Counsel and Privacy Officer, Erie Insurance Group

cc: Maria T. Vullo, Superintendent
Scott Fischer, Executive Deputy Superintendent, Insurance Division
Stephen Doody, Deputy Superintendent for Property & Casualty

iiabny
Independent Insurance Agents & Brokers of New York, Inc.
Trusted Choice

NYIA
New York Insurance Association, Inc.

PIA
Professional Insurance Agents