555 12th Street, NW
Suite 550
Washington, DC 20037
202-828-7100
Fax 202-293-1219
www.aiadc.org

December 17, 2018

Director Bruce R. Ramge, Chair
Mr. Jim Mealer, Vice Chair
Market Conduct Examination Standards (D) Working Group
NAIC Central Office
1100 Walnut, Suite 1500
Kansas City, MO 64106-2197

Attn: Petra Wallace, Market Regulation Specialist

VIA Electronic Mail: pwallace@naic.org

RE: Additional Comments on the New Insurance Data Security Pre-Breach Checklists for Inclusion in the Market Regulation Handbook

Dear Director Ramge and Mr. Mealer:

The American Insurance Association (AIA) appreciates the continued dialogue related to the National Association of Insurance Commissioners' (NAIC) draft Insurance Data Security Pre- & Post-Breach Checklists (Checklists) for inclusion in the Market Regulation Handbook (Handbook). The background and explanations on committee calls has been very helpful and we provide the following additional feedback for your consideration.

AIA recognizes and supports the regulators' responsibility and need to review an insurer's information security program taking into consideration the risk-based characteristics of these programs. On the November 30th call of Market Conduct Examination Standards (D) Working Group (Working Group), it was noted that pre-examination of insurance data security is typically covered in the financial exam, but due to budget and staffing constraints uniformity is not an objective that the handbook or leadership can provide definitive guidance on. As such the pre-breach checklist can serve as a reference document for those states that perform cyber examinations as part of the market conduct exam.

After further consideration, while we understand and appreciate the challenges to create uniformity, we believe that it is a worthwhile and important effort to encourage pre-breach assessments to be performed as part of the Financial Examination. We believe this approach would foster rather than harm corporate resiliency for the following reasons:

(1) **Efficiency:** The IT Examination component of the financial examination is a robust review that has incorporated the security elements of the Insurance Data Security Model Law and was recently amended to ensure there were no gaps related to the Model Law. Further, the financial exam is a review of the whole organization, so it provides a better understanding of the company's security

practices. Additionally, reviewing pre-breach security measures as part of the market conduct examination and the IT portion of the financial examination makes a lot of the pre-exam examination work redundant. The market conduct pre-breach checklist is also redundant to the annual certification that licensees must file as part of the Model Law requirements. The IT examination portion of the Financial Examination should be the sole vehicle for examining pre-breach security measures.

(2) **Expertise:** Arguably the individuals conducting the market conduct exam will not have the same expertise that those performing the IT examination do. This raises timing concerns, because key personnel could be taken away from core resiliency efforts to explain processes and procedures to unfamiliar examiners. This concern becomes elevated in the instance that there are several states performing cyber reviews as part of their market conduct examination process on the same group of companies in a given year. Now integral IT security personnel could be pulled away multiple times to explain the same processes and procedures. Finally, some Departments may hire special contractors to perform cyber reviews thereby resulting in unnecessary expenses that increase the cost of an examination that ultimately is redundant.

(3) **Coordination:** **C**onsistency in the examination framework is essential to avoid duplication and inconsistent examination standards for the same system with the same legal expectations in a risk-based environment. As such, the Financial examination process creates greater efficiency for companies and regulators.

(4) **Scope**: Market conduct examinations are directed at how the insurer interacts with consumers and agents reviewing primarily underwriting and claim handling practices. Security can have a consumer angle, but that is in a post-breach situation and in that context we can understand why a market conduct exam may be conducted to ensure all notification requirements were met in a timely manner.

We appreciate the recommendation to incorporate the guidance into Section 20 of the handbook, but, respectfully, feel that this is misplaced. Chapter 20 on its face appears to be the right fit given its review of the operations and management of the insurer, but it is our understanding that this review is for purposes of understanding the structure of the insurer and its operations to get a better understanding of the examinee not necessarily to duplicate the financial examination review.

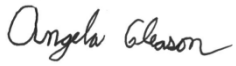
(5) **Adaptability:** We can't stress enough that cybersecurity cannot be a checkbox exercise. Companies need to create risk-based programs that are adaptable to the rapidly evolving nature of the threat and technology solutions. Unfortunately, the yes/no checkbox tool used by the market conduct examination does not support a flexible risk-based program. In our August 15th comment letter we identified some of the problems and concerns that yes/no questions raise.

(6) **Confidentiality:** The confidentiality and protection of information in this context is critical. Consideration should be given as to what examination method provides the strongest confidentiality protections.

For these reasons, we respect the effort and diverse regulatory needs, but urge the Working Group to eliminate a pre-breach checklist for inclusion in the market conduct exam. Instead, it may be useful to understand the current cyber examination landscape and survey the states to determine which states rely on the Market Conduct, Financial Exam, other examination tool, or combination of all of the above. This information can help create an examination framework that promotes resiliency and meets regulator needs.

AIA appreciates the opportunity to provide additional feedback and remains committed to a constructive and collaborative dialogue. Our feedback on the post-breach checklist can be found in our August 15th letter. Please let us know if you have any questions or if we can be of any further assistance.

Respectfully submitted,



Angela Gleason
Senior Counsel