American Insurance Association

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

August 15, 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: New Insurance Data Security Pre- & Post-Breach Checklists for Inclusion in the Market Regulation Handbook

Dear Director Ramge and Mr. Mealer:

The American Insurance Association (AIA) appreciates the opportunity to provide comments on the National Association of Insurance Commissioners' (NAIC) draft Insurance Data Security Pre- & Post-Breach Checklists (Checklists) for inclusion in the Market Regulation Handbook (Handbook). AIA was very active in the development of the Insurance Data Security Model Law (Model Law) and it is with that background that we provide the comments outlined below.

Consistency with the IT Examination

As a threshold matter, we are unclear as to the objective for including these Checklists in the Market Conduct Examination Handbook. In our experience, this issue has been primarily an IT Examination issue. Over the past few years, the NAIC's IT Examination Working Group has updated the IT Examination Handbook Guidance and we believe intends to also do so with regard to the Model Law. There is some overlap conceptually with the proposed Checklist items. Additionally, the IT Examiners have the expertise that market conduct examiners may not have to review the issues identified in the checklist.

We strongly urge consistency in the Examination frameworks and to avoid duplication that would unnecessarily complicate an already robust review. We believe that identifying the objectives of the Market Conduct review will assist in a more complete assessment as to the appropriate tool for reviewing a Licensee's Information Security Program and the substantive contents of the Checklist.

Advisory Language

We understand the Working Group's desire to proactively develop the Checklists, but respectfully urge the Working Group to wait to incorporate the Insurance Data Security Model Law until there is a better understanding of the role of the Market Conduct review and how states are going to incorporate the Model

Law into their state statutes. For example, Appendix B identifies 72-hr notice to the Commissioner or Director of Insurance as a criterion for review. At this time, the 72-hr requirement is only in 2 states; however, there are a handful of other states with existing laws that have varying timing requirements for notifying the Commissioner.

We acknowledge that throughout the Handbook there are references to compliance with NAIC Model Laws and that the Instructions and specific Handbook wording advise jurisdictions that they should closely review the handbook to determine the standards that reflect the statutes and regulations of the given jurisdiction and those that do not. We believe that it is important for the Working Group to reinforce this advisory language in this section as well and encourage jurisdictions to remove Appendix A and B from their individual jurisdiction's procedural manuals, if they have not adopted the Model Law.

Risk-Based

An important element of the model law is that the measures and practices identified in the Model Law are to be implemented based on the individual Licensee's risk assessment. This is a critical element of the Model Law that should be identified in the Review Guidelines and Instructions sections, because every item identified in the checklist may not be appropriate for every Licensee and will not be implemented in the same manner as other companies. In many instances a "yes" or "no" response may not be a good indicator of compliance. Additionally, this is another reason that the IT Examination may be a better resource for regulators.

Specific Recommendations

We have also identified the following criteria in the proposed Checklists that are not part of the Model Law. Notably, some of the specifics identified below are not specified in the Model Law because they depend on an individual company risk analysis and implementation decision and are not conducive to the prescriptive approach some of these criteria take. These are our initial observations and look forward to providing additional insight, as appropriate.

Exhibit A - Pre-Breach Checklist

- Criteria 3, 4 and 5: The Model Law requires that an Information Security Program be developed, implemented and maintained by the Licensee's Executive Management and reported on annually. Nowhere in the Model Law is there a requirement that the Board, IT Steering Committee, or Executive Management approve of the Information Security Program. Additionally, there is no reference in the Model Law to an IT Steering Committee. The Board can delegate some of its authority to a committee; however, it should not be assumed that such delegation is to an IT Steering Committee.

  As such, we recommend the following amendments.
  3. Has the ISP been reviewed ~~and approved~~ by the Licensee's executive management?
  4. Has the overall status of the ISP been ~~reviewed and approved by~~ reported to the Licensee's Board of Directors?
  ~~5. Has the ISP been reviewed and approved by the Licensee's IT Steering Committee?~~

- Criterion 6: The Model Law does not identify a specific timing requirement for review. As such this question is beyond the scope of the Model Law and given the risk-based nature of the Model Law will not be meaningful.

- Criterion 7: This criterion suggests that a description is required of the roles and responsibilities of any function of the information security program that is outsourced to a third party and how the Licensee will oversee such third party. This is not required by the Model Law. Rather, the Model Law requires that the Licensee designate persons/third parties who are responsible for the information

security program, and separately requires that the Licensee oversee third party service provider arrangements, generally. Requiring that Licensees include this detailed information about third party responsibilities for the Information security program functions potentially puts Licensees at risk of having such information exploited by bad actors. This is another example of where a "yes" or "no" answer is not always appropriate, but at the same time a detailed description may also be concerning. Careful consideration should be given as to how the IT Examination handles this type of question and whether there is any unnecessary and troublesome duplication.

- Criterion 10: Again, there is no requirement in the model to regularly communicate to the employees. If this is intended to assess training, that issue seems to be addressed in criterion 12.

- Criterion 13: There is no requirement as to the specific intervals at which cyber-awareness training should occur.

- Criteria 21 and 22: Importantly, due to a risk-focused approach, the Model does not require the Licensee to include information security standards as part of its contracts with third-party services providers. It also does not require inspections or reviews of the Third Party's Information Security Practices. Instead the Model Law requires the Licensee to exercise due diligence and, under the overarching umbrella of risk analysis, as applicable, require the Third Party to implement appropriate administrative, technical, and physical measures. A more consistent criterion would be to ask if the Licensee has a process to conduct due diligence according to the risk of the third party.

- Criterion 24: It is not a bad practice for a company to have guidance in place as to when to institute a Cybersecurity Event investigation, but again this is beyond the scope of the model and should be implemented based on the Licensee's risk assessment.

- Criterion 27: Section 4(H)(2)(f) generally requires that the Response Plan address the documentation and reporting of a Cybersecurity Event. This is a very different requirement than what is identified in the Checklist as requiring a written assessment of the nature and scope of the event. As appropriately identified in the Model Law, it should be the Licensee's decision as to how the Response Plan addresses documenting and reporting the Events. A company may not want to have a written assessment of the nature and scope of the Cybersecurity Event for security reasons. Therefore, the Criterion could inadvertently add a requirement to the Model Law that hinders rather than promotes security.

- Criterion 29: Similarly, Section 4(H)(2)(e) has a general requirement that Response Plan address remediation efforts. This is very different then identifying clear steps to be taken to restore the security of a compromised information system. Cyber events are not always the same and again having clear steps to be taken may lessen corporate resiliency.

- Criterion 30: We cannot find any obligation in the Model Law for the incident Response Plan to address steps to be taken when a Cybersecurity Event occurs at a Third Party Service Provider.

- Criterion 31: This criterion adds a requirement that incident Response Plan provide *detailed* instructions for the external and internal communications and information sharing. Nowhere in Section 4 is there a requirement for detailed instructions.

- Criteria 33 and 34: These criteria should be in the incident Response Plan section only. Additionally, the requirement identified in 34 is not reflective of the Model Law. The Model Law states that the incident Response Plan should address "the evaluation and revision, *as necessary,* of the incident Response Plan following a Cybersecurity Event.

Post-Breach Checklist

- Criterion 3: As stated earlier, the timing requirement for notifying a regulator of a breach varies among states and as such this criterion should be more generic.

- Criterion 4i: The notification does not need to include an estimate of the number of customers globally affected.

- Criterion 4j: Not all internal reviews of automated controls need to be included, but rather those identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed.

- Criterion 6: Currently, not every state requires a Licensee to provide a copy of the notice to the Commissioner/Director.

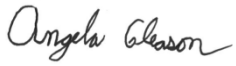
- Criterion 8: This criterion appears to distinguish between independent producers and producers of record, the Model Law does not appear to do this.

- Criterion 10: This Criterion appears to make what is a discretionary "make available" provision in the Model Law a requirement. Additionally, there may be some security concerns associated with including this type of information.

****

AIA appreciates the opportunity to provide feedback and remains committed to a constructive and collaborative dialogue. We respectfully ask that the Working Group consider whether the Checklists are the appropriate vehicle for regulatory review at this time and welcome the opportunity to provide additional substantive feedback, as appropriate. Please let us know if you have any questions or if we can be of any further assistance.

Respectfully submitted,



Angela Gleason
Senior Counsel

