American Property Casualty Insurance Association
INSURING AMERICA apci.org

March 6, 2019

Director Bruce R. Ramge, 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: Insurance Data Security Pre-Breach Checklists for Inclusion in the Market Regulation Handbook

Dear Director Ramge:

The American Property Casualty Insurance Association (APCIA)[1] 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). During the December 19th conference call it was indicted that Working Group would begin to review the substantive contents of the pre- and post-breach checklists and develop language to encourage market regulators to coordinate with domestic financial regulators. We provide the following feedback to assist in this review process.

Checklists

Consistent with APCIA's understanding of the objective for these checklists and a review of the Model Law, we respectfully recommend the following changes:

Pre-Breach Checklist

Information Security Program (Sections 4A and 4B)
Review Criteria

Proposed Amendments to Draft Checklist	Reason for Amendments
1. Does the Licensee have a written Information Security Program (ISP)?	
2. Does the ISP clearly state the person(s) at the Licensee responsible for the program?	

[1] Representing nearly 60 percent of the U.S. property casualty insurance market, the American Property Casualty Insurance Association (APCIA) promotes and protects the viability of private competition for the benefit of consumers and insurers. APCIA represents the broadest cross-section of home, auto, and business insurers of any national trade association. APCIA members represent all sizes, structures, and regions, which protect families, communities, and businesses in the U.S. and across the globe.

Proposed Amendments to Draft Checklist	Reason for Amendments
3. Has the ISP been reviewed and approved by the Licensee's executive management?	The Model Law requires that an ISP 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 ISP. 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.
4. Has the overall status of the ISP been ~~reviewed and approved by~~ reported to the Licensee's Board of Directors? (Section 4E)	
~~5. Has the ISP been reviewed and approved by the Licensee's IT steering committee?~~	
~~6. How often is the ISP reviewed and updated? (Section 4G)~~	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.
7. ~~Are any functions of the ISP outsourced to third parties? (if Yes, identify any such providers, review their roles and responsibilities, and the Licensee's oversight of the third parties.)~~	The Model Law requires that the Licensee designate persons/third parties who are responsible for the ISP and separately requires that the Licensee oversee third party service provider arrangements, generally. Requiring that Licensees include detailed information about third party responsibilities for the ISP through this checklist is concerning for the following reasons: (1) such detailed disclosure in this document potentially puts Licensees at risk of having such information exploited by bad actors; (2) this is an issue that is addressed through the IT examination and careful consideration should be given as to whether this is truly necessary for the objectives of the market conduct guidance; and (3) implementation of 3rd party oversight is addressed later-on in the checklist.
~~8. Does the ISP contain appropriate administrative, technical and physical safeguards for the protection of Nonpublic Information and the Licensee's Information Systems ?~~	This question should be moved to the next section of the checklist, which addresses components of the ISP.
9. Does the Licensee stay informed regarding emerging threats and vulnerabilities? (Section 4D(4))	
10. ~~Does the Licensee regularly communicate with its employees regarding security issues?~~	There is no requirement in the model to regularly communicate with employees. Additionally, "security issues" is a vague term. A Licensee would not want to communicate to employees about "issues" related to weaknesses in the Licensee's controls, security incidents, etc. If instead the question is directed at training, that topic is addressed in question 12.
11. Does the Licensee ensure that employee's hardware is updated on a timely basis to ensure necessary security software updates and patches have been downloaded and installed?	
12. Does the Licensee provide cybersecurity awareness training to its personnel? (Section 4D(5))	
~~13. How soon after onboarding a new employee does the Licensee provide cybersecurity awareness training? At what intervals is the training renewed?~~	The Model Law does not identify a specific interval at which cyber-awareness training should occur. Also, it does not require training at on-boarding. Question 12 should be sufficient and any additional review should be coordinated with the IT examiner.

Proposed Amendments to Draft Checklist	Reason for Amendments
14. Does the Licensee utilize reasonable security measures when sharing information? (Section 4D(4))?	
15. Has the Licensee conducted a Risk Assessment to identify foreseeable internal and external threats to its information security?	
16. When was the last Risk Assessment conducted or updated?	
17. Has the Licensee designed its ISP to be adjusted as appropriate based on ~~address issues identified in~~ its Risk Assessment?	As drafted this questions implies that all issues found in a Risk Assessment should be addressed. In fact, that is not the objective of the Model Law, which is risk-based. Accepting risk is often an appropriate method for handling risk. We believe the recommended edit more accurately aligns with Section 4(G)'s requirement for program adjustments.
18. Are Cybersecurity Risks included in the Licensee's Enterprise Risk Management process? (Section 4D(3))	

Components of Information Security Program (Section 4D and 4F)

Proposed Amendments to Draft Checklist	Reason for Amendments
8. Based on the Licensee's risk assessment does the ISP contain ~~appropriate~~ administrative, technical and physical safeguards for the protection of Nonpublic Information and the Licensee's Information Systems ?	As noted above, Question 8 appears to be more closely aligned with this section of the checklist, which focuses on the components of an ISP In addition, APCIA respectfully recommends that "appropriate" be replaced by a reference to the risk assessment. The NAIC Model Law is risk-based and "appropriate" is a broad term without any direction as to what that might be interpreted to mean.
19. Has the Licensee determined that the following security measures are appropriate and ~~has the Licensee~~ implemented them as part of its ISP? (If NO for any items, coordinate with the IT examiner to understand why such measures were not implemented, and as necessary, interview the appropriate responsible Licensee's personnel ~~to discuss the reason(s) such measures were not implemented~~.)	A review of security measures is a prime example where coordination with the domestic regulator's IT examiners will serve to promote efficiency and, as such, enhance corporate resiliency. Arguably the individuals conducting the market conduct exam will not have the same expertise that those performing the IT examination do. Further, the IT examiner has likely already performed a robust examination of what security measures have and have not been implemented and the reasons for these decisions. Finally, starting with the IT examiner will avoid taking key personnel away from core resiliency efforts to explain processes and procedures to unfamiliar examiners.
19a. Access controls to limit access to Information Systems to Authorized Individuals?	
19b. Physical controls on access to Nonpublic Information to limit access to Authorized Individuals.	
19c. Protection of Nonpublic Information by encryption or other appropriate means while being transmitted externally or stored on portable computing devices or media?	
19d. Secure development practices for in-house applications and procedures for testing the security of externally developed applications?	

Proposed Amendments to Draft Checklist	Reason for Amendments
19e. Controls for individuals accessing Nonpublic Information such as Multi-Factor Authentication?	
19f. Regular testing and monitoring of systems to detect actual and attempted attacks or intrusions into Information Systems?	
19g. Audit trails in the ISP to detect and respond to Cybersecurity Events and permit reconstruction of material financial transactions?	
19h. Measures to prevent Nonpublic Information from physical damage, loss or destruction due to environmental hazards?	The addition of "due to environmental hazards" is consistent with the Model Law language.
19i. Secure disposal procedures for Nonpublic Information?	

Third-Party Service Providers (Section 4F)

Proposed Amendments to Draft Checklist	Reason for Amendments
20. Does the Licensee have Third-Party Service Providers with which it shares Nonpublic Information?	
21. Does the Licensee have a process to exercise third-party service provider due diligence according to the risk the third-party presents ~~include information security standards as part of its contracts with such providers~~?	Importantly, due to a risk-focused approach, the Model Law does not require the Licensee to include information security standards as part of its contracts with third-party service providers. It also does not require inspections or reviews of the Third Party's Information Security Practices. Instead, the Model Law requires a 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.
~~22. Does the Licensee conduct inspections or reviews of its providers' information security practices?~~	

Incident Response Plan (Section 4H)

Proposed Amendments to Draft Checklist	Reason for Amendments
23. Does the ISP contain a written incident response plan and/or detailed process for responding to a Cybersecurity Event?	
~~24. Does the incident response plan provide clear guidance on when to initiate a Cybersecurity Event investigation?~~	It is not a bad practice for a company to have guidance in place as to when to institute a Cybersecurity Event investigation, but this is beyond the scope of the Model Law and should be implemented based on the Licensee's risk assessment.
25. Does the incident response plan contain a list of clear and well-defined objectives?	
26. Does the Incident response plan provide clear roles, responsibilities and levels of decision-making authority?	
27. Does the incident response plan address the documentation and reporting of a Cybersecurity Event ~~require written assessment of the nature and scope of a Cybersecurity Event~~?	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

Proposed Amendments to Draft Checklist	Reason for Amendments
	documenting and reporting the Events. A Licensee may not want to have a written assessment of the nature and scope of the Cybersecurity Event for security reasons. Therefore, the question could inadvertently add a requirement to the Model Law that hinders rather than promotes security.
28. Does the incident response plan require determination of whether any Nonpublic Information was exposed during a Cybersecurity Event and to what extent?	
29. Does the incident response plan address remediation ~~provide clear steps to be taken to restore the security of any information systems compromised in a Cybersecurity Event~~?	Section 4(H)(2)(e) has a general requirement that a 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 having clear steps to be taken may lessen corporate resiliency.
~~30. Does the incident response plan sufficiently address steps to take when a Cybersecurity Event occurs at a Third-Party Service Provider where data provided by the Licensee is potentially at risk?~~	This is not a requirement in the Model Law.
31. Does the incident response plan provide ~~detailed~~ instructions for external and internal communications and ~~as well as~~ information sharing ~~with regulatory authorities~~?	Nowhere in Section 4 is there a requirement for "detailed" instructions. In addition, 4(H)(2)(d) requires addressing external and internal communications and information sharing generally.
32. Does the incident response plan define various levels of remediation based on the severity of identified weaknesses?	

Documentation and Reporting

Proposed Amendments to Draft Checklist	Reason for Amendments
~~33. Does the ISP describe documentation and reporting procedures for Cybersecurity Events and related incident response activities (Section 4H)~~	This is unnecessary and redundant to questions 23 through 32.
~~34. Does the ISP require a post-event evaluation following a Cybersecurity Event? (Section 4H)~~	This is not required by the Model Law. Rather the Model requires that the Incident Response Plan should address the evaluation and revision of such plan, *as necessary*.
35. Does the ISP require retention of all records related to Cybersecurity Events for a minimum of five years? (Section 5D)	
36. Has the Licensee prepared and submitted annual certifications to its domiciliary state Commissioner/Director of Insurance (Section 4(H))	

Prior Examination Findings

Proposed Amendments to Draft Checklist	Reason for Amendments
~~37. Has the Licensee addressed and implemented corrective actions to material findings from any prior examinations?~~	Given how rapidly technology and the threat landscape evolves, this question may be unnecessary or moot.

Post-Breach Checklist

Post-Event Investigation by Licensee (Section 5)

Proposed Amendments to Draft Checklist	Reason for Amendments
1. Did the Licensee conduct a prompt investigation of the Cybersecurity Event? (Section 5A)	
2. Did the Licensee ~~appropriately~~ determine the nature and scope of the Cybersecurity Event? (section 5B)	As noted above "appropriately" is a broad term with no clear standard associated with it. We recommend deleting this term.

Notice to Commissioner/Director of Insurance (Section 6)

Proposed Amendments to Draft Checklist	Reason for Amendments
3. Did the Licensee provide timely notice ~~(no later than 72 hours)~~ to the Commissioner or Director of Insurance following a Cybersecurity Event? (Section 6A)	Notification to the Commissioner/Director vary by state and as such this question should be more generic.
4. Did the Notification to the Commissioner or Director of Insurance include the following information, to the extent reasonably available? (Section 6B)	
4a. The date of the Cybersecurity Event, or the date upon which it was discovered?	
4b. A description of how the Nonpublic Information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of Third-Party Service Providers, if any?	
4c. How the Cybersecurity Event was discovered?	
4d. Whether any lost, stolen or breached Nonpublic Information has been recovered, and if so, how this was done?	
4e. The identity of the source of the Cybersecurity Event?	
4f. Whether the Licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies? (If YES, did the Licensee provide the date(s) of such notification(s)?)	
4f. A description of the specific types of Nonpublic Information acquired without authorization?	
4h. The period during which the Information System was compromised by the Cybersecurity Event?	
4i. A best estimate of the number of total Consumers in this state ~~and globally~~ affected by the Cybersecurity Event?	The Model Law does not address the number of individuals globally affected.
4j. The results of any internal review ~~of automated controls and internal procedures and whether or not such controls and procedures were followed~~ identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed?	This question has been modified to conform to the Model Law.
4k. A description of efforts being undertaken to remediate the circumstances which permitted the Cybersecurity Event to occur?	
4l. A copy of the Licensee's privacy policy and a statement outlining the steps the Licensee will take to investigate the Cybersecurity Event and to notify affected Consumers?	

Proposed Amendments to Draft Checklist	Reason for Amendments
4m. The name of a contact person familiar with the Cybersecurity Event and authorized to act for the Licensee?	
5. Did the Licensee provide timely updates to the initial notification and Questions 4a-4m above? (Section 6B)	

Proposed Amendments to Draft Checklist	Reason for Amendments
6. Did the Licensee provide timely and sufficient notice of the Cybersecurity Event to Consumers? (If YES, and as appropriate, did the Licensee provide a copy of the notification to the Commissioner(s)/Directors of all affected states?) (Section 6C)	Not every state requires the Licensee to provide a copy of the notice to the Commissioner/Director.
7. Did the reinsurer Licensee provide timely and sufficient notice of the Cybersecurity Event to ceding insurers? (Section 6E)	
8. Did the Licensee provide timely and sufficient notice of the Cybersecurity Event to independent insurance producers ~~and/or producers~~ of record of affected Consumers? (Section 6F)	The Model Law obligation is to notify insurance producers of record.

Proposed Amendments to Draft Checklist	Reason for Amendments
9. Did the Cybersecurity Event occur at a Third-Party Service Provider (If Yes, did the Licensee fulfill its obligations to ensure compliance with this law, either directly or by the Third-Party Service Provider?) (Section 5C and 6D)	

Proposed Amendments to Draft Checklist	Reason for Amendments
~~10. What changes if any are being considered to the Licensee's ISP as a result of the Cybersecurity Event and the Licensee's response?~~	This question appears to make what is a discretionary "make available" provision in the Model Law a requirement. Additionally, there could be security concerns associated with this type of information.

Introductory Language

Based on the last Working Group call, APCIA respectfully recommends that additional introductory language be added to: (1) clearly identify when the pre-breach checklist should be utilized; (2) further emphasize the need for consultation with domestic financial examiners to leverage the IT examination; and (3) highlight that the data security model is risk-based and that a risk-based analysis will underlie all decisions made by Licensees.

****

Thank you for your continued collaboration. If you have any questions or would like to discuss any of these recommendations further, please let us know.

Respectfully submitted,

Angela Gleason and Alex Hageli