MARKET REGULATION HANDBOOK
INSURANCE DATA SECURITY PRE-BREACH AND POST-BREACH CHECKLISTS

Company Name	
Period of Examination	
Examination Field Date	
Prepared By	
Date	

GUIDANCE

NAIC Insurance Data Security Model Law (#668)

Note: The guidance that follows should only be used in states that have enacted the *NAIC Insurance Data Security Model Law (#668)* or legislation which is substantially similar to the model. Moreover, in performing work during an exam in relation to the Model Law, it is important the examiners first obtain an understanding and leverage the work performed by other units in the department including but not limited to financial examination- related work.

OVERVIEW

The purpose and intent of the Insurance Data Security Model Law is to establish standards for data security and standards for the investigation of and notification to the Commissioner or Director of Insurance of a Cybersecurity Event affecting Licensees.

REVIEW GUIDELINES AND INSTRUCTIONS

When reviewing a Licensee's Information Security Program for compliance with the Insurance Data Security Model Law (NAIC Model #668) for the prevention of a Cybersecurity Event as defined in the model law, please refer to the examination checklist attached as Exhibit A hereto.

When reviewing a Licensee's Information Security Program and response to a Cybersecurity Event for compliance with the Insurance Data Security Model Law subsequent to a suspected and/or known Cybersecurity Event as defined in the model law, please refer to both examination checklists attached as Exhibits A and Exhibit B hereto.

When considering whether to undertake such a review, refer to Section 9 of NAIC Model #668, which provides certain exceptions to compliance for Licensees with fewer than ten employees; Licensees subject to the Health Insurance Portability and Accountability Act (Pub.L, 104-191, 110 Stat. 1936, enacted August 21, 1996); and certain employees, agents, representatives, or designees of Licensees who are in themselves Licensees.

Exhibit A: Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 4

INFORMATION SECURITY PROGRAM (Sections 4A and 4B)

REVIEW CRITERIA	NOTES *(YES, NO, NOT APPLICABLE, OTHER)*
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?	Section 4.C.(1)
3. Has the ISP been reviewed ~~and approved~~ by the Licensee's executive management?	Edited language
4. Has the overall status of the ISP been reviewed ~~and approved~~ by the Licensee's Board of	Section 4.E.(2)(a)
~~5. Has the ISP been reviewed and approved by the Licensee's IT steering committee?~~	Remove, as inapplicable
6. ~~How often is the ISP reviewed and updated?~~Has the Licensee monitored, evaluated and adjusted, as appropriate, the Information Security Program consistent with any relevant changes in technology, the sensitivity of its Nonpublic Information, internal or external treats to information, and the Licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to Information Systems?	Section 4.G.
7. Does the Licensee Grant Oversight of the ISP by Third-Party Service Provider Arrangements? Does the Licensee designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the Licensee who is responsible for the ISP? ~~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.*)~~	Section 4.C.(1) See also Criterion 21 & 22, per Section 4.F.
8. Does the ISP contain appropriate administrative, technical and physical safeguards commensurate with the size and complexity of the Licensee and the nature and scope of the Licensee's activities? ~~for the protection of Nonpublic Information and the Licensee's Information Systems?~~	
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?~~	N/A per the Model See Criteria 12 below.
~~11. Does the Licensee ensure that employees' hardware is updated on a timely basis to ensure necessary security software updates and patches have been downloaded and installed?~~	See Criteria 6, as amended, above.
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?~~	N/A, there is no requirement as to the specific intervals at which cyber-awareness training should occur in the Model.
14. Does the Licensee utilize reasonable security measures when sharing information? (Section 4D(4))	

Commented [EM1]: 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 to the left:

Exhibit A: Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 4

RISK ASSESSMENT (Section 4C)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT APPLICABLE, OTHER)***
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~~? Has the Licensee implemented information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assessed the effectiveness of the safeguards' key controls, systems, and procedures?	Section 4.C.(5)
17. Has the Licensee designed its ISP to address issues identified in its Risk Assessment?	
18. Are Cybersecurity Risks included in the Licensee's Enterprise Risk Management process? (Section 4D(3))	

COMPONENTS OF INFORMATION SECURITY PROGRAM (Section 4D)

REVIEW CRITERIA	**NOTES *(YES, NO, NOT***
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 item, interview the appropriate responsible personnel to discuss the reason(s) such measures were not implemented.)*	
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~~ over an external network or stored portable computing devices or media?	Section 4.D.(2)(d)
19d. Secure development practices for in-house applications and procedures for testing the security of externally developed applications?	
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?	
19i. Secure disposal procedures for Nonpublic Information?	

Exhibit A:

Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist
for Operations/Management Standard #17
Insurance Data Security Model Law #668, Section 4

THIRD-PARTY SERVICE PROVIDERS (Section 4F)

REVIEW CRITERIA	NOTES *(YES, NO, NOT APPLICABLE, OTHER)*
20. Does the Licensee have Third-Party Service Providers with which it shares Nonpublic Information?	
21. Does the Licensee exercise due diligence in selecting its Third-Party Service Provider? ~~Does the Licensee include information security standards as part of its contracts with such providers?~~	Per Section 4.F.(1)
22. Does the Licensee require a Third-Party Service Provider to implement appropriate administrative, technical, and physical measures to protect and secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider?~~. Does the Licensee conduct inspections or reviews of its providers' information security practices?~~	Per Section 4.F.(2)

INCIDENT RESPONSE PLAN (Section 4H)

REVIEW CRITERIA	NOTES *(YES, NO, NOT APPLICABLE, OTHER)*
23. Does the ISP contain a written incident response plan and/or ~~detailed~~ process for responding to a Cybersecurity Event?	Section 4.H.(1)
24. Is the Licensee's written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event that compromises the confidentiality, integrity, or availability of Nonpublic Information in its possession? ~~Does the incident response plan provide clear guidance on when to initiate a Cybersecurity Event investigation?~~	Section 4.H.(1)
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 documentation and reporting regarding Cybersecurity Events and related incident response activities?~~Does the incident response plan require written assessment of the nature and scope of a Cybersecurity Event?~~	Section 4.H.(2)(f)
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~~ Is the incident response plan ~~provide clear steps to be taken to restore the security of any information systems compromised in a~~designed for the Licensee to promptly recover from any Cybersecurity Event? Does the incident response plan address identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls?	Section 4.H.(1) Section 4.H.(2)(e)
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?~~	No Requirement in Model.
31. Does the incident response plan address external & internal communications & information sharing? ~~Does the incident response plan provide detailed instructions for external and internal~~	Section 4.H.(2)(d)
32. Does the incident response plan identify requirements for ~~define various levels of~~ remediation of any identified weaknesses in Information Systems and associated controls? ~~based on the severity of identified weaknesses?~~	Section 4.H.(2)(e)

Commented [EM2]: 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

Exhibit A: Supplemental Incident Response Plan Readiness (Pre-Breach) Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 4

DOCUMENTATION AND REPORTING

REVIEW CRITERIA	NOTES *(YES, NO, NOT APPLICABLE, OTHER)*
33. Does the ISP describe documentation and reporting ~~procedures for~~regarding Cybersecurity Events and related incident response activities? (Section 4.H.(f))	Section 4.H.(2)(f)
34. Does the ISP require ~~a post-event evaluation following a Cybersecurity Event?~~the evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.	Section 4.H.(2)(g)
35. Does the ISP require retention of all records related to Cybersecurity Events for a minimum of five years from the date of the Cybersecurity Event?	Section 5.D.
36. Has the Licensee prepared and submitted annual certifications to its domiciliary state Commissioner/Director of Insurance? (Section 4I)	

PRIOR EXAMINATION FINDINGS

REVIEW CRITERIA	NOTES *(YES, NO, NOT APPLICABLE, OTHER)*
37. ~~Has the Licensee addressed and implemented corrective actions for any material findings from any prior examinations?~~To the extent an insurer has identified areas, systems, or processes that require material improvement, updating or redesign, has the insurer documented the identification and the remedial efforts planned and underway to address such areas, systems or processes?	There is no reference in the Model to "corrective actions to any material findings from any prior examinations". Replaced with language from Section 4.I.

Exhibit B: Supplemental Incident Response Plan Investigation (Post-Breach) and Notification Cybersecurity Event Checklist for Operations/Management Standard #17 Insurance Data Security Model Law #668, Section 5 and 6

POST-EVENT INVESTIGATION BY LICENSEE (Section 5)

REVIEW CRITERIA	NOTES *(YES, NO, NOT APPLICABLE, OTHER)*
1. Did the Licensee conduct a prompt investigation of the Cybersecurity Event?	Section 5.A.
2. Did the Licensee assess ~~appropriately determine~~ the nature and scope of the Cybersecurity Event?	Section 5.B.(2)

NOTICE TO COMMISSIONER/DIRECTOR OF INSURANCE (Section 6)

REVIEW CRITERIA	NOTES *(YES, NO, NOT APPLICABLE, OTHER)*
3. Each Licensee shall notify the Commissioner as promptly as required under applicable state law, but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred when either of the following criteria has been met: ~~Did the Licensee provide timely notice (no later than 72 hours) to the Commissioner or Director of Insurance following the Cybersecurity Event?~~	Per Section 6.A. (1) & (2), at least one of two criteria must be met for the threshold for notice to the Commissioner to be triggered.
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, or the Licensee became aware of the Cybersecurity Event?	
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)?)*~~And, if so, when such notification was provided.	Section 6.B.(6).
4g. A description of the specific types of information ~~Nonpublic Information~~ acquired without authorization?	The defined term "Nonpublic Information" was not used in Section 6.B.(7)
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 number or best estimate of total Consumers in this State affected by the Cybersecurity Event.	The notification is not required to include an estimate of the number of customers globally affected. Replaced with language from Section 6.B.(9).
4j. ~~The results of any internal review of automated controls and internal procedures and whether or not such controls and procedures were followed~~? The results of any internal review identifying a lapse in either automated controls or internal procedures or confirming that all automated controls or internal procedures were followed.	Not All internal reviews of automated controls are required to be included, but rather those identifying a lapse in either automated controls or internal procedures. Per Section 6.B.(10).
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?	
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)	

OTHER NOTIFICATIONS (Section 6)

REVIEW CRITERIA	NOTES *(YES, NO, NOT APPLICABLE, OTHER)*
6. ~~Did the Licensee provide timely and sufficient notice of the Cybersecurity Event to Consumers? (*If YES, did the Licensee provide a copy of the notification to the Commissioner(s)/Directors of all affected states?*)~~ Did the Licensee comply with [insert state's data breach notification law], as applicable, and provide a copy of the notice sent to Consumers under that statute to the Commissioner, when the Licensee is required to notify the Commissioner under Section 6A?	Section 6.C.
7. ~~Did the reinsurer Licensee provide timely and sufficient notice of the Cybersecurity Event to ceding insurers~~? If applicable, did the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of making the determination that a Cybersecurity Event has occurred as required under applicable state law?	Section 6.E.(1)(a)
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~~? In the case of a Cybersecurity Event that involved Nonpublic Information in the possession, custody or control of a Licensee that is an insurer or its Third-Party Service Provider and for which a Consumer accessed the insurer's services through an independent insurance producer, did the insurer notify the producers of record of all affected Consumers as soon as practicable as directed by the Commissioner. (Unless the insurer is excused from this obligation because it did not have the current producer of record information for any individual Consumer).	Section 6.F.

THIRD PARTY SERVICE PROVIDERS

REVIEW CRITERIA	*NOTES (YES, NO, NOT APPLICABLE, OTHER)*
9. Did the Cybersecurity Event occur at a Third-Party Service Provider? If yes, did the Licensee fulfill its obligations under this law? ~~(*If YES, did the Licensee fulfill its obligations to ensure compliance with this law, either directly or by the Third-Party Service Provider?*)~~	

POST-EVENT ANALYSIS

REVIEW CRITERIA	*NOTES (YES, NO, NOT APPLICABLE, OTHER)*
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~~? Did the Licensee adjust, as appropriate, the Information Security Program consistent with any relevant changes in technology, the sensitivity of its Nonpublic Information, internal or external threats to information, and the Licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to Information Systems.	Section 4.I.