NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

MEMORANDUM

TO: Cynthia Amann, Chair of the Cybersecurity (H) Working Group

FROM: Judy Weaver, Facilitator of the Chief Financial Regulator Forum

DATE: August 16, 2024

RE: Data Security Model Compliance Testing

During its August 12, 2024, meeting, the Chief Financial Regulator Forum discussed whether and how testing for compliance with the Insurance Data Security Model Law (NAIC #668) should be incorporated into full-scope financial condition examinations. In addition, the group discussed whether and how any findings associated with such compliance testing should be communicated across states.

Now that many states have adopted Model #668 or similar requirements (25 as of Spring 2024), as well as the significant amount of overlap between Model compliance testing and what is typically covered in a financial exam IT Review, many states have begun incorporating some compliance testing procedures into their financial examinations. In fact, the IT Examination (E) Working Group has developed a mapping between Model #668 compliance requirements and the IT Review procedures included in the NAIC's *Financial Condition Examiners Handbook* to assist in synchronizing test procedures in this area (see **Attachment A**).

In many cases, states conducting Model #668 compliance test procedures include their findings in a regulator-only management letter as opposed to the public report of examination, due to the sensitivity of IT security topics. Such management letters are generally posted to the regulator-only Financial Examination Electronic Tracking System (FEETS) in iSite+ for sharing with other states.

However, the practices of conducting Model #668 compliance testing procedures and reporting results in a management letter are not consistently applied across all states and are not codified as clear expectations for the lead/domestic state to perform in financial examination guidance.

Additionally, some states may be conducting Model #668 compliance testing procedures on licensed companies through market conduct examinations, given related guidance incorporated into the NAIC's *Market Regulation Handbook*. The lack of clear guidance and expectations for compliance testing and reporting responsibilities has the potential to lead to overlap and duplication of efforts across states and functions.

As the Cybersecurity (H) Working Group is charged with supporting the states with implementation efforts related to the adoption of Model #668, the Chief Financial Regulator Forum is referring these issues for your consideration. For example, questions that could be answered by the Working Group include, but are not limited to, the following:

- Should Model #668 compliance test procedures be incorporated into each full-scope financial condition examination where at least one licensed state has adopted Model #668 or similar requirements?
- Should Model #668 findings be incorporated into regulator-only management letters (or similar communication tools) with the results shared across all licensed states?

Once policy decisions have been made in these areas, we recommend that they be communicated to other relevant NAIC groups for implementation (i.e., IT Examination (E) Working Group, Market Conduct Examination Guidelines (D) Working Group).

If there are any questions regarding the referral, please contact either me or NAIC staff (Bruce Jenson at *bjenson@naic.org*) for clarification. Thank you for your consideration of this important issue.

NOTE: This document is designed as a resource for examiners to use in finding related procedures between the Model Law and Exhibit C. Risk statements and procedures should be customized depending on the situation of the company. This tool should only be used in states that have enacted the *NAIC Insurance Data Security Model Law* (#668). 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 Market Conduct related work.

Model Law Ref. #	Model Law - General Description	Exhibit C Ref. #	Risk Statement	Control/Test Procedure
D(1)	IT structure/program appropriate to support business activities.	APO 01	IT organizational structure is inadequate to support business objectives.	(Multiple)
D(2)a	Access Controls - Place access controls on Information Systems, including controls to authenticate and permit access only to Authorized Individuals to protect against the unauthorized acquisition of Nonpublic Information;	DSS 05.04	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	(Multiple)
		APO 10	Third-party service provider risks are not properly assessed, addressed, and mitigated.	The company has a formal process in place whereby: 1) Risk is assessed based on the company's understanding of the third-party service providers information security program as well as by the company's ability to verify elements of the third-party service provider's security program; 2) Based on the company's risk, the company ranks vendors and uses a vendors ranking to determine depth and frequency of review procedures performed related to ongoing vendor relationships; 3) The company determines appropriate access rights, based on the risk assessment and company needs; 4) The company designs specific mitigation strategies, including network monitoring specific to third-party service providers and **access controls**, where appropriate.
D(2)b	Managing Personal Data - Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;	APO 03	Enterprise goals may not be met because the data and systems architecture is poorly defined and/or fragmented.	The company has an information architecture model that addresses the creation, use and sharing of data between applications that maintain data integrity, flexibility, functionality, cost-effectiveness, timeliness, security and availability.
		DSS 05.01	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	(Multiple)
D(2)c	Physical access - Restrict access at physical locations containing Nonpublic Information, only to Authorized Individuals;	DSS 05.05	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	Procedures are defined and implemented to grant, limit and revoke access to premises, buildings and areas, according to business needs, including during emergencies.
D(2)d	Data encryption - Protect by encryption or other appropriate means, all Nonpublic Information while being transmitted over an external network and all Nonpublic Information stored on a laptop computer or other portable computing or storage device or media;	DSS 05.02	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	Sensitive data is exchanged only over a trusted path or medium, with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin.
		DSS 05.07	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	The company has an established company-wide IT security baseline and periodically tests and monitors its IT security implementation for compliance with that baseline. Protection against data leaks are implemented
D(2)e	Application Security - Adopt secure development practices for in-house developed applications utilized by the Licensee and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Licensee;	BAI 01	IT projects may fail to meet business objectives/ERM goals or run over budget in the absence of an effective program and project-management methodology.	A methodology exists to maintain the portfolio of projects that includes identifying, defining, evaluating, prioritizing, selecting, initiating, managing and controlling projects.
		BAI 03.05	Project deliverables fail to meet business objectives due to inadequate design and/or ineffective oversight of implementation.	(Multiple)
		APO 03	Enterprise goals may not be met because the data and systems architecture is poorly defined and/or fragmented.	The company has an information architecture model that addresses the creation, use and sharing of data between applications that maintain data integrity, flexibility, functionality, cost-effectiveness, timeliness, security and availability.
D(2)f	Compliance with Information Security Program - Modify the Information System in accordance with the Licensee's Information Security Program;	BAI 06&07	A lack of proper change management threatens system stability and/or integrity.	The company has a process in place to record, authorize, manage, monitor and implement requests for changes. Procedures exist to ensure documentation is appropriately updated and distributed to affected users and IT staff upon completion of change.
D(2)g	Authentication Procedures - Utilize effective controls, which may include Multi-Factor Authentication procedures for any individual accessing Nonpublic Information;	DSS 05.04	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	User identities are enabled via authentication mechanisms including multi-factor authentication for remote access, as appropriate based on the sensitivity of the information which may be accessed.
D(2)h	System Monitoring - Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, Information Systems;Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, Information Systems;	DSS 05.07	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	The company has an established company-wide IT security baseline and periodically tests and monitors its IT security implementation for compliance with that baseline.
D(2)i	Audit Trails - Include audit trails within the Information Security Program designed to detect and respond to Cybersecurity Events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Licensee;	DSS 01.03	The quality, timeliness and availability of business data is reduced due to an ineffective data-management process.	IT infrastructure activity is logged with sufficient detail to reconstruct, review and examine operational activities; this activity is monitored on a regular basis.
		DSS 03.01&02	The company has an ineffective problem-management process that increases operating costs and reduces system availability, service levels and customer satisfaction.	The company maintains problem-management policies and procedures, including escalation triggers, with adequate audit trails and analysis to identify, report and classify incidents by category, impact, urgency and priority.
				The company has implemented a problem-management system that identifies and initiates solutions addressing the root cause of the problem and provides adequate audit trail facilities that allow tracking, analyzing and determining the root cause of all reported problems.
D(2)j	Environmental Hazards - Implement measures to protect against destruction, loss, or damage of Nonpublic Information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures: and	DSS 01.04	Inadequate physical and environmental controls may result in unauthorized access and inadequate protection of data.	The data center contains proper physical and environmental controls to protect the equipment, data and personnel located within.
		DSS 04.07	Inadequate continuity management may result in the inability to ensure critical business functions.	All critical backup media, documentation and other IT resources necessary for IT recovery and continuity plans are stored off-site in a secure location.
D(2)k	Information Disposal - Develop, implement, and maintain procedures for the secure disposal of Nonpublic Information in any format.	DSS 05.06	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	Procedures are in place to ensure that business requirements for protection of sensitive data and software are met upon disposal or transfer of data and hardware (endpoints, mobile devices, network devices, servers, portable media and hard drives).
D(3)	ERM Intergation - Include cybersecurity risks in the Licensee's enterprise risk management process.	APO 12	IT-related enterprise risks have not been integrated into the overall enterprise risk management (ERM) program.	(Multiple)

Model Law Ref. #	Model Law - General Description	Exhibit C Ref. #	Risk Statement	Control/Test Procedure
D(4)	Emerging Threats - Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and	DSS 05.07	The company's business is threatened by the impact of operational information security vulnerabilities and incidents.	Threat and vulnerability information received from information-sharing forums and sources (e.g., Financial Services Information Sharing and Analysis Center, etc.) is used in developing a risk profile.
D(5)	Provide cybersecurity training - Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the Licensee in the Risk Assessment.	APO 01	IT organizational structure is inadequate to support business objectives.	Review training programs and schedules to confirm that management and employees are provided with sufficient training to understand the importance of compliance with IT and cybersecurity policies, including awareness of concepts of phishing, malware, and data loss prevention, as appropriate.
E(1)	Require the Licensee's executive management or its delegates to develop, implement, and maintain the Licensee's Information Security Program	APO 01	IT organizational structure is inadequate to support business objectives.	The company's IT management organizational structure, with clearly defined roles and responsibilities, supports business objectives and IT priorities and enables efficient decision making.
E(2)a	Annual reporting of the overall status of the Information Security Program and the Licensee's compliance with this Act	MEA 03	IT processes and IT-supported business processes are not compliant with applicable laws, regulations, and other contractual requirements.	A procedure has been implemented to review and report compliance of IT policies, standards, procedures and methodologies with applicable legal and regulatory requirements.
E(2)b	Annual reporting of material matters related to the Information Security Program, addressing issues such as risk assessment, risk management and control decisions, Third-Party Service Provider arrangements, results of testing, Cybersecurity Events or violations and management's responses thereto, and recommendations for changes in the Information Security Program.	MEA 01	The company does not properly identify and address IT performance and conformance deficiencies.	The company has adopted and implemented a formalized monitoring framework to define the scope, methodology and process to be followed for measuring IT's solution, service delivery and contribution to the company, including tracking corrective actions to address anomolies.
E(3)	If executive management delegates any of its responsibilities under Section 4 of this Act, it shall oversee the development, implementation and maintenance of the Licensee's Information Security Program prepared by the delegate(s) and shall receive a report from the delegate(s) complying with the requirements of the report to the Board of Directors above.	APO 01	IT organizational structure is inadequate to support business objectives.	The company's IT management organizational structure, with clearly defined roles and responsibilities, supports business objectives and IT priorities and enables efficient decision making.
F(1)	A Licensee shall exercise due diligence in selecting its Third-Party Service Provider	APO 10	Third-party service provider risks are not properly assessed, addressed, and mitigated.	The company has a formal process in place whereby: 1) Risk is assessed based on the company's understanding of the third-party service providers information security program as well as by the company's ability to verify elements of the third-party service provider's security program; 2) Based on the company's risk, the company ranks vendors and uses a vendors ranking to determine depth and frequency of review procedures performed related to ongoing vendor relationships; 3) The company determines appropriate access rights, based on the risk assessment and company needs; 4) The company designs specific mitigation strategies, including network monitoring specific to third-party service providers and **access controls**, where
F(2)	A Licensee shall 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	APO 10	Third-party service provider risks are not properly assessed, addressed, and mitigated.	The company has a formal process in place whereby: 1) Risk is assessed based on the company's understanding of the third-party service providers information security program as well as by the company's ability to verify elements of the third-party service provider's security program; 2) Based on the company's risk, the company ranks vendors and uses a vendors ranking to determine depth and frequency of review procedures performed related to ongoing vendor relationships; 3) The company determines appropriate access rights, based on the risk assessment and company needs; 4) The company designs specific mitigation strategies, including network monitoring specific to third-party service providers and **access controls**, where appropriate.