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.