NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Attachment #2
IT Examination WG 6-12-26 Comments

MEMORANDUM

TO: Brett Bache (RI), Chair, Market Conduct Examination Guidelines (D) Working Group

FROM: Ber Vang (CA), Chair, Information Technology Examination (E) Working Group
Shane Mead (KS), Vice Chair, Information Technology Examination (E) Working Group

DATE: June 12, 2026

RE: Comments for the Cybersecurity Event Response Coordination Framework

On behalf of the Information Technology Examination (E) Working Group, we want to express our support for the proposed Cybersecurity Event Response Coordination Framework. We believe that the framework establishes a much-needed structured approach for coordinating the efforts of insurance regulators responding to cybersecurity events of national significance in the insurance sector. Identifying a Coordinating Lead State to facilitate the regulatory response makes sense as this will help reduce the number of inquiries that the regulated entity will receive and possibly reduce the number of resources non-lead state regulators will need to monitor and/or respond to the cybersecurity event.

As mentioned in the exposure draft, the framework operates within a larger context that includes other NAIC documents, laws, and regulations. The framework references specifically three NAIC documents/projects that play a central role relative to responding to cybersecurity events, including the Cybersecurity Event Response Plan, the Cybersecurity Response Coordination Framework, and the Cybersecurity Event Notification Portal (portal). We do not have any suggested changes to the proposed framework, but we do want to bring to your attention a potential problem regarding the portal and its role within the Cybersecurity Response Coordination Framework. The portal's purpose is to streamline how regulated entities report cyber incidents to state regulators by allowing those entities to securely submit a standardized, one-to-many event notification to multiple states at once and similarly provide updates to their breach reports. Although the portal is still in development, as it is currently contemplated the portal will be accessible only by state regulators whose jurisdiction has adopted the NAIC Insurance Data Security Model Law (Model #668). We believe this restriction could potentially hamper the implementation of the Cybersecurity Event Response Coordination Framework, as states that have not adopted Model #668 will still require their regulated entities to provide notifications and updates separately to those states.

In addition, the following scenarios and questions may need some consideration and/or explicit guidance to address:

- In a scenario in which the Coordinating Lead State for a cybersecurity event has not adopted Model #668, but other regulators in the group have adopted it, will the Coordinating Lead State's inability to share updates on the state's response through the portal be a problem?
- Will information shared during conference calls include all information posted to the portal that would otherwise be inaccessible to states that have not adopted Model #668, or will some information be selectively reserved for only the Model #668 states?
- Will a lead state's absence of Model #668 adoption explicitly disqualify that state from acting in the capacity of Coordinating Lead State for purposes of the proposed framework if another state regulator in the group has adopted Model #668?

While we understand that some of the concerns above may need to be addressed by the Cybersecurity (H) Working Group, we believe that consideration and workarounds for them are necessary to ensure smooth implementation of the framework.

The Information Technology Examination (E) Working Group is open to exploring and adding any necessary guidance to the Financial Condition Examiners Handbook to support the Cybersecurity Event Response Coordination Framework.