601 Pennsylvania Avenue, NW
South Building, Suite 500
Washington, D.C. 20004
T 202.778.3200
F 202.331.7487
ahip.org

July 24, 2026

Petra Wallace
Market Conduct Examination Guidelines (D) Working Group
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106-2197

By Email to: Petra Wallace at Pwallace@NAIC.org

Re: NAIC Market Conduct Examination Guidelines (D) Working Group exposure of Cybersecurity Event Response Coordination Framework

Dear Ms. Wallace:

On behalf of AHIP[1], thank you for the opportunity to provide feedback on the proposed Cybersecurity Event Response Coordination Framework (Framework).

We understand that the Working Group's objective in developing the Framework is to enhance coordination efforts in response to cybersecurity events of national significance in the insurance industry, and appreciate the potential benefits associated with greater consistency and predictability in multi-state regulatory responses. In reviewing the exposure, there are several areas identified where more clarity and direction would be helpful. We have highlighted those below.

Assign Lead State as Primary Point of Contact. The Framework should explicitly state that, upon activation, the Lead State will serve as the primary regulatory point of contact with the affected regulated entity (Entity), and that participating states will channel information requests and related communications through the Lead State rather than contacting the Entity independently. Without that clarification, the Framework could add a new coordination layer on top of existing multi-state demands rather than meaningfully reducing duplicative requests.

Explicitly Address Confidentiality Protections. The Framework does not address how confidential information shared by the Entity will be protected as it moves from the Lead State to participating states and NAIC staff. It should clarify that information shared under the Framework will be handled consistent with applicable confidentiality protections under Model #668 and relevant state examination or investigative confidentiality laws, including appropriate limits on further disclosure and use.

Define Scope. The catch-all provision stating that within scope will be "any situation in which regulators deem that this Framework would benefit the work of state insurance regulators" effectively removes any meaningful activation threshold. The Framework should include defined minimum criteria, such as the number of affected states or policyholders or a demonstrated cross-jurisdictional impact, to reserve activation for cybersecurity events of national or multi-state significance.

Address Engagement of Regulated Entities. The Framework does not contemplate notice of activation to an Entity, nor does it provide an opportunity for Entity input before violation findings or corrective actions are determined. A framework that allows regulators to determine violations and corrective actions without corresponding notice and input could raise fairness and procedural concerns.

Define Role of Participating States. Section 4 gives the Lead State responsibility for determining whether violations occurred and what corrective action is appropriate. The Framework does not address how participating states would concur in or adopt those findings, whether the findings would be binding, or what happens if states disagree. Without that clarity, an Entity could face a Lead State finding in addition to independent enforcement from participating states. The Framework should address the intended effect of Lead State determinations on other states' enforcement authority.

Address Regulated Entity Obligations Under Existing Laws. The Framework does not address how it interacts with existing breach-notification timelines, including the 72-hour requirement under Model #668, ongoing state examinations, or parallel federal and law-enforcement investigations. It should clarify that activation does not create new or accelerated notification obligations beyond those imposed by applicable law, and it should explain how the Lead State and participating states are expected to coordinate with other regulators and law-enforcement authorities to minimize conflicting or duplicative directives.

Account for Critical Regulated Entity Processes After an Event. As the Working Group develops the Framework and any related regulatory requirements, it should recognize the non-regulatory obligations an Entity faces after a cybersecurity incident. Any regulatory requirements should avoid interfering with essential investigation, containment, and remediation efforts in the immediate aftermath of an incident. The Framework should balance the need for timely incident reporting with the operational demands of an incident response.

Thank you for the opportunity to submit these important considerations. We look forward to continued collaboration through the development of a Framework that will serve both regulators and regulated entities.

Sincerely,
LaCosta Wix
AHIP Senior Regulatory Counsel, State Affairs and Policy

Cc: Miranda Motter, Senior Vice President, State Government Affairs and Policy

[1]AHIP is the national association whose members provide health care coverage, services, and solutions to hundreds of millions of Americans every day. We are committed to market-based solutions and public-private partnerships that make health care better and coverage more affordable and accessible for everyone. Visit www.ahip.org to learn how working together, we are Guiding Greater Health.