American Property Casualty Insurance Association℠
INSURING AMERICA apci.org

July 24, 2026

NAIC Market Conduct Examination Guidelines (D) Working Group
NAIC Central Office
1100 Walnut Street
Suite 1500
Kansas City, MO 64106
Via email: pwallace@naic.org

RE: Cybersecurity Event Response Coordination Framework

Dear Chair Bache and Members of the Market Conduct Examination Guidelines (D) Working Group:

Thank you for the opportunity to provide comments on the proposed Cybersecurity Event Response Coordination Framework (the "Framework"). APCIA[1] supports the NAIC's focus on strengthening coordination among state insurance regulators and enhancing preparedness for cybersecurity events of potential national significance. Improving communication, consistency, and efficiency in multi-state regulatory responses is an important objective.

At the same time, it is essential that the Framework remain appropriately scoped as a coordination mechanism among regulators, rather than evolving, intentionally or in practice, into an additional layer of oversight or a centralized supervisory construct. Maintaining this distinction will be critical to ensuring the Framework is legally sound, operationally practical, and consistent with existing regulatory authorities and established reporting frameworks.

We believe the NAIC should take sufficient time to carefully consider the scope, structure, sequencing, and safeguards associated with the Framework before moving toward implementation. In particular, its relationship to existing initiatives, most notably the Cybersecurity Event Notification Portal, and to current reporting regimes warrants further development. Absent clear integration and sequencing, there is a risk that the Framework could introduce duplication, inconsistent expectations, or additional operational burden in an already complex environment. Recent events further underscore both the sensitivity of cybersecurity-related information and the considerations and risks that arise when significant volumes of insurer data are aggregated. These dynamics highlight the importance of ensuring that any approach to information sharing is deliberate, well-defined, and appropriately limited.

[1] The American Property Casualty Insurance Association (APCIA) is the primary national trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA represents the broadest cross-section of home, auto, and business insurers of any national trade association. APCIA membership consists of over 1,200 member companies (or over 300 member groups). APCIA member companies P&C countrywide market share is 65% (total 73% commercial lines, 55% personal lines).

American Property Casualty Insurance Association℠
INSURING AMERICA apci.org

With these considerations in mind, we respectfully offer the following comments.

Confidentiality, Legal Authority, and NAIC Role

Our primary concern is the potential direct or indirect expansion of access to insurers' confidential incident information and the role contemplated for the NAIC.

Insurers report cybersecurity events under established statutory frameworks, including laws modeled on the NAIC Insurance Data Security Model Law (IDSM), which carefully limit access and protect confidentiality. The Framework should not expand access beyond regulators with clear legal authority or create pathways for broader dissemination to jurisdictions that would not otherwise have regulatory authority.

The Framework should also avoid positioning the NAIC as a centralized repository, clearinghouse, or independent analytical body for insurer-specific incident data. Centralizing sensitive information in this manner could introduce additional cybersecurity risk, create ambiguity around data ownership and control, and raise questions regarding the scope of the NAIC's authority.

Clear guardrails are needed to ensure that information sharing remains subject to existing legal protections and jurisdictional limits, that the NAIC's role is confined to facilitating coordination among authorized regulators, and that the Framework does not result in any direct or indirect expansion of access to confidential insurer data beyond those jurisdictions determined to be in-scope under their existing laws and regulations.

Information Flow, Scope, and Coordination

Greater clarity is needed on how cybersecurity events are introduced into the Framework, how information flows among regulators, and how insurer-provided data may be shared across jurisdictions. It remains unclear whether state-submitted notifications will be transmitted to the NAIC or more broadly disseminated, and whether this could create indirect reporting obligations, duplicative requests, reporting in jurisdictions whose IDSM enactment was not triggered in an incident, or inconsistent communication channels.

Without clear parameters, insurers could face parallel inquiries from multiple regulators, undermining efficiency and diverting resources from incident response. The Framework should preserve and reinforce established reporting channels with domiciliary and authorized regulators and should not create new or duplicative pathways, explicitly or implicitly.

Further clarity is also needed on core definitional elements, including:

- ensuring that "cybersecurity event" is not given broader scope than under state enactments,
- the threshold for events of "national significance," and

American Property Casualty Insurance Association℠
INSURING AMERICA apci.org

- the scope of the catch-all provision "any situation in which regulators deem that this Framework would benefit the work of state insurance regulators."

Absent clearly defined triggers, thresholds, and limiting principles, there is a risk of inconsistent application, unnecessary escalation, and expansion of the Framework beyond its intended purpose.

Alignment with Existing Regulatory Frameworks

The Framework should be designed to operate within, not on top of, the existing regulatory landscape. Insurers today must navigate a complex, multi-jurisdictional framework with variations in reporting thresholds, timing requirements, and regulatory authorities, often compounded by overlapping obligations. In this context, it is important that the Framework streamline coordination and reduce duplication, rather than introduce additional procedural or supervisory layers.

The Framework also does not clearly address how it would interact with existing legal and regulatory obligations, including breach-notification timelines, ongoing state examinations, and parallel federal or law-enforcement investigations. It should clarify that activation of the Framework does not create new or accelerated notification obligations beyond those required by applicable law and should describe how participating regulators will coordinate with other authorities to avoid conflicting or duplicative inquiries or directives.

Continued progress toward broader adoption of the Insurance Data Security Model Law across states would further support these objectives by promoting greater consistency in reporting standards, definitions, and regulatory expectations. A more uniform baseline framework would enhance the effectiveness of coordination by reducing variability and uncertainty across jurisdictions. Also, it is important that states enacting an IDSM-inspired law recognize that many states have passed such laws, making it exceedingly difficult, if not impossible, for licensees navigating multi-jurisdictional incidents to report to every jurisdiction within a few days. As such, more reasonable reporting timeframes are necessary to ensure that licensees can remain appropriately focused on incident containment, mitigation and other response efforts.

Alignment with the Cybersecurity Event Notification Portal is also critical, especially as the Portal remains under development and its final scope and functionality are not yet fully defined. Advancing the Framework without a clear understanding of how it will integrate with or depend on the Portal risks creating duplicative processes and uncertainty. A more sequenced approach would better support effective implementation.

Operational Impact and Supervisory Approach

The Framework should emphasize proportionality and a risk-based approach to information requests, particularly in the early stages of an event, and should align with existing reporting requirements to minimize burden.

As drafted, there is a risk that the Framework could be interpreted as creating an expectation of escalated supervisory activity, including market conduct or financial examinations. It is important to clarify that cybersecurity events do not automatically trigger examinations, and any supervisory response should remain discretionary, risk-based, and case-specific.

The Framework also provides limited clarity regarding the insurer's role once coordination is activated, including whether insurers will receive notice, understand what information is being shared and with whom, and have an opportunity to provide input before information is shared or findings or corrective actions are considered. Greater transparency regarding these processes would promote consistency, accountability, and confidence in the Framework.

Similarly, the Framework should clearly establish that coordination, once activated, should occur through a disciplined structure, such as a Coordinating Lead State, to minimize duplicative or inconsistent requests. The Framework would also benefit from greater clarity regarding the role and authority of the Coordinating Lead State and how participating states are expected to act on coordinated findings or recommendations. Without such clarity, insurers could face inconsistent outcomes despite the existence of a coordinated process.

Coordination and information requests should also be structured to avoid interfering with an insurer's ability to contain, remediate, and respond to the incident in a timely manner.

Information Sharing Across States

Clarification is needed regarding the extent to which information may be shared with non-affected states, or states where the incident does not meet statutory notification triggers, including the legal basis for such sharing and the associated confidentiality protections. An event that is reportable in one jurisdiction may not be reportable in another, and expanding visibility without clear authority or need could create inefficiencies, compromise confidentiality and incident response efforts, and divert attention from regulators with direct oversight responsibility.

The Framework should ensure that participation and access are appropriately limited to regulators with a defined role and clear legal authority in connection with the event.

Conclusion

Appropriately scoped coordination can improve consistency and support effective responses to significant cybersecurity events. Achieving these objectives will depend on maintaining a clear focus on coordination, not oversight, and avoiding expansion of authority, new reporting layers, or uncertainty in roles.

The Framework should build on existing reporting structures, reinforce established regulatory relationships, provide clear governance regarding information sharing and decision-making, align with related initiatives such as the Cybersecurity Event Notification Portal, and include appropriate limits on

American Property Casualty Insurance Association℠
INSURING AMERICA apci.org

information access and use. It should also be developed in a deliberate and measured manner that reflects the complexity and sensitivity of the current environment.

Accordingly, we encourage the NAIC to take the time necessary to address stakeholder concerns regarding scope, safeguards, and operational impact before advancing the Framework. Doing so will help avoid unintended consequences and better position the Framework to achieve its intended objectives.

We appreciate the NAIC's leadership and welcome continued dialogue.

Thank you,

Kristin Abbott
Sr. Director and Counsel, Cyber & Privacy Issues

Lisa Brown
Assistant Vice President, Market Conduct & Counsel

