July 24, 2026

Brett Bache, Chair
Danielle Torres, Vice Chair
Market Conduct Examination Guidelines (D) Working Group
National Association of Insurance Commissioners
1100 Walnut Street Kansas City, MO 64106-2197

Submitted via email: pwallace@naic.org

RE: Comments on the Draft Cybersecurity Event Response Coordination Framework

Dear Chair Bache and Vice Chair Torres:

The Blue Cross Blue Shield Association (BCBSA) appreciates the opportunity to comment on NAIC's draft Cybersecurity Event Response Coordination Framework. As cyber threats continue to target the healthcare sector, it is increasingly important that regulatory coordination efforts support effective incident response and recovery. We support efforts to streamline reporting and coordination efforts to reduce burdens on these necessary functions.

BCBSA is a national federation of independent, community-based and locally operated Blue Cross and Blue Shield companies (Plans) that collectively cover, serve and support 1 in 3 Americans. BCBS Plans contract with 95% of hospitals and 91% of doctors across the country and serve those who are covered through Medicare, Medicaid, an employer, or purchase coverage on their own.

BCBSA supports NAIC's goal of improving coordination among state insurance regulators during significant cybersecurity events. We also appreciate NAIC's efforts to ensure a collaborative process where industry can contribute to and comment on this framework. Industry engagement ensures the framework reflects real-world incident response challenges. This framework has the potential to reduce duplicative regulatory requests, improve consistency across states, and allow affected entities to focus resources on response, remediation, member protection, and continuing business operations during an active incident. However, cybersecurity events often involve highly sensitive legal, financial, and health-related information that must be appropriately protected throughout the coordination process. The framework must also be scoped to support, rather than hinder, ongoing response and recovery efforts by avoiding unnecessary burdens, conflicting expectations, or duplicative requests that could divert

resources away from remediation activities needed to protect consumers and maintain critical healthcare operations.

BCBSA offers the following recommendations to help ensure the framework operates as a practical coordination tool that supports regulators, protects patients and consumers, safeguards sensitive and proprietary information and enables affected entities to focus resources on incident response, recovery, and the timely restoration of critical healthcare operations.

1. **BCBSA recommends NAIC establish clear activation criteria that focuses on material impacts, reserving the framework for significant cybersecurity events.**

   The draft framework identifies several factors regulators may consider when determining whether an event warrants a coordinated response, including the nature of the event, the number of policyholders affected, the number of states involved, and the operational impact on the affected company. However, the current criteria remain largely qualitative and are not tied to a clear materiality threshold, making it hard to determine when the framework will be activated. We recommend the framework be reserved for significant cybersecurity events involving actual or likely material impacts and not be triggered for routine incidents that can be effectively managed through existing regulatory processes. This focuses resources on the incidents that are tied to true risk for patients and where coordinated regulatory engagement is necessary and likely to improve regulatory oversight or consumer protection outcomes.

   BCBSA recommends that activation decisions be based on objective indicators of actual or likely material impact, such as significant operational disruption, harm to consumers, or substantial multi-state implications, rather than the mere possibility that an event could become significant. Greater clarity regarding the factors used to activate the framework would help regulators and affected entities develop a common understanding of when coordinated regulatory engagement is warranted, improve consistency across states, provide greater predictability during incident response, and enable affected entities to focus resources on containment and recovery efforts. In turn, this would help reduce disruptions that can affect patients, providers, and access to care.

2. **BCBSA recommends NAIC establish clear decision-making timelines.**

   We recommend establishing target timelines for key decision points, including the initial evaluation of an event, the recommendation by the Cybersecurity (H) Working Group to active the framework, the notification to committee leadership, and the designation of a Coordinating Lead State. Clearly defined decision-making timelines would promote greater consistency and improve planning where coordinated regulatory engagement is necessary. This clarity would allow affected entities to focus resources on incident response and recovery rather than navigating uncertainty about regulatory expectations, helping to reduce operational disruptions that can affect providers, patients, and access to care.

3. **BCBSA recommends that NAIC provide clarity on the criteria used to select a Coordinating Lead State.**

   The draft framework identifies several factors that may be considered when selecting a Coordinating Lead State, including premium volume, domicile, operational presence, and expertise. However, it provides limited insight into how those factors will be evaluated or weighed in practice. BCBSA recommends that NAIC provide additional transparency regarding how the selection criteria will be applied and how unique circumstances may be considered when determining the most appropriate Lead State for a particular event.

   Greater transparency in the selection process would improve predictability for regulators and affected entities, support more efficient coordination, and support a common understanding of roles and responsibilities during a cybersecurity event. Clear expectations regarding Lead State selection can also help reduce confusion, facilitate information sharing, and enable all parties to focus on timely response and remediation efforts.

4. **BCBSA recommends that NAIC address cybersecurity events affecting insurers that originate from other entities in the healthcare ecosystem.**

   Large-scale cybersecurity incidents increasingly involve interconnected healthcare ecosystems where multiple organizations may be impacted by a single event. The current framework is largely structured around incidents involving regulated entities (i.e., the insurer themselves) and provides limited guidance regarding how a coordinated response would operate when the compromised organization is a third party. In these situations, the scope and impacts of an incident are often not immediately known, and affected entities may receive additional information over time as investigations progress. Depending on the nature of the event, a third party may be responsible for certain notifications or reporting obligations, while insurers may have separate obligations related to impacts on their own operations, members, or data.

   BCBSA recommends that NAIC establish a clear process for evaluating cybersecurity events that originate outside the insurer and involve multiple affected entities. This will avoid duplicative reporting, inconsistent information sharing, and confusion during an active incident. The framework should clarify expectations around, lines of responsibility, and information sharing processes among the affected entities while acknowledging that information regarding the scope and impacts of an incident often develops over time. Because third parties and insurers may have distinct reporting obligations and responsibilities, clear expectations are necessary to avoid duplicative reporting, inconsistent information sharing, and confusion during active incident response.

   Without this guidance, regulators may receive information on different timelines from multiple affected entities as the scope and impacts of an incident continue to evolve. This can make it more difficult to develop a complete understanding of the event, may

generate duplicative information requests, and could divert resources away from response and remediation activities that are necessary to protect consumers and maintain critical healthcare operations. Establishing clear coordination expectations would support more effective regulatory oversight while facilitating timely response efforts during complex, multi-party cybersecurity incidents.

5. **BCBSA recommends aligning the framework with existing state and federal reporting requirements.**

   Health insurers already operate under a complex network of state and federal cybersecurity, privacy, breach notification, and operational reporting requirements. During an active cybersecurity event, organizations are often required to respond simultaneously to state insurance regulators, federal agencies, law enforcement, providers, customers, and other stakeholders. As currently drafted, the framework could create duplicative reporting requests or overlapping regulatory inquiries at the very time organizations must prioritize incident response and recovery.

   BCBSA recommends that NAIC clearly describe how the framework will operate alongside existing regulatory requirements, including state cybersecurity notification laws, the Insurance Data Security Model Law (#668), HIPAA breach notification requirements, the NAIC Cybersecurity Event Notification Portal, the NAIC Cybersecurity Event Response Plan, and other applicable state and federal reporting requirements, including those involving state attorneys general and federal agencies with overlapping jurisdiction. The framework should make clear that participation does not establish new reporting obligations beyond those required under applicable law and should, whenever possible, follow a "report once, use many times" approach that minimizes duplication and reduces unnecessary administrative burden during active incident response.

   This approach would help promote consistent information sharing across regulators, reduce the risk of conflicting or duplicative reporting requests, and allow affected entities to focus resources on incident containment, remediation, and consumer protection. Without greater alignment across regulatory requirements, organizations may be required to respond to multiple inquiries covering similar information on different timelines, potentially diverting resources from response and recovery efforts. Clear coordination among state and federal regulators would improve regulatory visibility into significant cybersecurity events while helping to ensure that patients and consumers receive timely protections and that critical healthcare operations remain uninterrupted.

6. **BCBSA recommends strengthening protections for sensitive cybersecurity information.**

   Effective regulatory coordination depends on maintaining the confidentiality of sensitive information shared during a cybersecurity incident. Incident response frequently involves highly sensitive technical, legal, and operational information, including forensic reports, threat intelligence, remediation plans, security vulnerabilities, and privileged communications. Unnecessary dissemination of evolving investigative information could

increase risk, interfere with ongoing response activities, compromise applicable privileges, or create additional cybersecurity exposure.

BCBSA recommends incorporating strong confidentiality, privilege, trade secret, and non-waiver protections throughout the framework. Information sharing should follow data minimization principles and be limited to information reasonably necessary to support the framework's coordination objectives. We further recommend that NAIC clarify how regulator-only communications will be protected and establish appropriate safeguards for forensic reports, threat intelligence, remediation plans, and attorney-client privileged communications shared during the course of a coordinated response. This structure will enable a more ready flow of the necessary information between stakeholders, making the framework more dynamic and successful.

7. **BCBSA recommends incorporating healthcare-specific considerations and federal coordination.**

   Cybersecurity incidents affecting health insurers can disrupt the delivery of healthcare. While the draft framework appropriately considers factors such as policyholder impact and premium volume, regulators should also consider operational impacts that affect patients, providers, and public programs, including disruptions to claims processing, provider reimbursement, pharmacy operations, Medicare and Medicaid administration, and patient access to care.

   These impacts are important because they may have significant consequences for consumers and the broader healthcare system even when traditional insurance-focused metrics—such as the number of policyholders affected or premium volume—do not fully reflect the severity of the event. Failure to account for healthcare-specific operational impacts could result in the underestimation of the significance of an incident or delaying coordinated action during events that materially affect patient access to care, provider operations, or the administration of public programs.

BCBSA appreciates NAIC's efforts to strengthen coordination among state insurance regulators during significant cybersecurity events. We believe the framework has the potential to improve regulatory communication and consistency; however, its success will depend on clear activation criteria, appropriate treatment of third-party incidents, alignment with existing reporting requirements, strong protections for sensitive information, and recognition of the unique operational challenges associated with healthcare cybersecurity events.

We appreciate the opportunity to provide these comments and look forward to continuing to work with NAIC as the framework evolves. We encourage continued stakeholder engagement as NAIC considers revisions to the framework which would help ensure the framework is practical, aligned with existing requirements, and effective in real-world cybersecurity incidents.

If you have any questions, please do not hesitate to contact Randi Chapman at randi.chapman@bcbsa.com.

Sincerely,

Clay S. McClure
Senior Director, State Affairs
Blue Cross Blue Shield Association