Cybersecurity Event Response Coordination Framework

1. Purpose, Scope, and Use of This Framework

Continuing cybersecurity events have directed a national spotlight on the need for a regulatory framework to enhance coordination efforts in response to cybersecurity events of national significance in the insurance sector.

The Market Regulation and Consumer Affairs (D) Committee, the Innovation, Cybersecurity and Technology (H) Committee, and the Financial Conditions (E) Committee have responsibility for developing standards and guidance on cybersecurity preparedness and post-incident actions of regulated entities.

This document recommends establishing a structured response framework built around a coordinating lead-state concept with support to be provided by several groups as suggested below. The document also concludes with several discussions aimed at driving regulator input on key design choices should a framework receive further consideration.

This framework includes detailed responsibilities for each committee, coordination mechanisms for complex events that cross jurisdictional boundaries, and specific implementation recommendations to formalize these procedures.

By establishing a structured approach, the NAIC can ensure consistent, effective responses to cybersecurity events while protecting both consumers and the stability of the insurance market.

2. Evaluation and Response Process

As cybersecurity events take place, the Cybersecurity (H) Working Group will evaluate events and will engage with domestic regulators to see if the events would benefit from a coordinated response. The evaluation will include consideration of the following criteria:

- Direct Premium Written for company impacted
- Nature of the event and type of data involved
- # of Policyholders affected

- # of States involved
- # of companies affected (in case where a singular event affects multiple entities)
- Operational impact to company affected
- Whether the company operates internationally and if so, how international regulators are responding

The criteria above are not intended to restrict state use of this Framework and its processes. Any situation in which regulators deem that this Framework would benefit the work of state insurance regulators or aid in supporting the protection of insurance policyholders could be within the scope of this framework.

Over the course of the year, NAIC staff will work with the Cybersecurity (H) Working Group (CWG) and other regulators to determine if any cybersecurity event could benefit from a coordinated response through the Framework, based on consideration of the criteria listed above.

After initial and preliminary information gathering, NAIC staff will provide an event summary to CWG.

NAIC staff, domestic regulators (as appropriate), and the CWG will work to:

1. Document a recommendation as to whether the Framework should apply for a given incident.
    a. The recommendation will summarize the event, explain the impact and reasoning to apply the framework, and will reach a preliminary assessment as to whether the event is one that should be treated primarily as a market conduct inquiry, financial inquiry, or as an industry event.
2. Communicate the recommendation to the leadership of the:
    a. Market Regulation and Consumer Affairs (D) Committee
    b. Financial Condition (E) Committee
    c. Innovation, Cybersecurity, and Technology (H) Committee
    d. Other Committee leadership as appropriate
3. Based on responses received, NAIC staff and CWG leadership will identify a coordinating lead state and work together to facilitate information sharing on the following:
    a. Market Conduct
        i. Examining consumer data exposure and notification requirements
        ii. Assessing market conduct implications
        iii. Reviewing compliance with privacy regulations
        iv. Coordinating multi-state market conduct examinations

v. Monitoring consumer complaint patterns
vi. Evaluating producer licensing impacts
vii. Developing consumer protection measures

b. Financial / Solvency Event – Assessment of financial impact
   i. Evaluating financial impact of the breach
   ii. Assessing capital adequacy implications
   iii. Reviewing business continuity capabilities
   iv. Assessing risk management systems
   v. Determining potential rating implications

c. Operational (Both) –
   i. Status of resolution for any remediation of operational impacts including monitoring claims-paying ability

The coordinating lead state will work with NAIC staff and CWG leadership to provide communication via:

- All state calls / calls among affected states
- Regulator only communications, and/or
- Summary response documentation providing with talking points in case of external inquiries as to how regulators are responding to the event

Communication and updates may consist of information explaining the cybersecurity event, impact to the insurer, impact to consumers, and may later provide insights on lessons learned as a result of responding to the cybersecurity event.

3. Coordinating Lead State Selection

Every insurance holding company system has individual characteristics that make it unique. Therefore, an evaluation of traits is required to determine how examinations responding to a cybersecurity event should be coordinated and which individual state, known as the Coordinating Lead State (Lead State), should assume the leadership role in a cybersecurity event response. The Lead State is leading the state insurance regulatory response primarily consisting of information gathering and dissemination of such information.

In most situations to date, a Lead State may have already been identified pursuant to the protocols overseen by either the Market Regulation and Consumer Affairs (D) Committee or the Financial Condition (E) Committee and any of their supporting groups. While deference should be given to previously selected Lead States, there may be circumstances driven by capacity or other circumstances where a different Lead State may need to be selected. Factors that may be considered when determining the Lead State are:

- State with the largest number of domestic insurance companies in the group.
- State of large or largest premium volume or exposure.
- Domiciliary state of top-tiered insurance company in an insurance holding company system.
- Physical location of the main corporate offices or largest operational offices of the group.
- Authority to take action and respond to the event including adoption of the Insurance Data Security Model Law (#668)
- Expertise in the area of concern and specialized experience of a state's staff members
- Ability to perform duties and responsibilities of a lead state

Because each company or group has its own unique characteristics and similar each cybersecurity event is unique, it may be appropriate to select a Lead State that differs from the Lead State otherwise selected for market or financial supervision purposes.

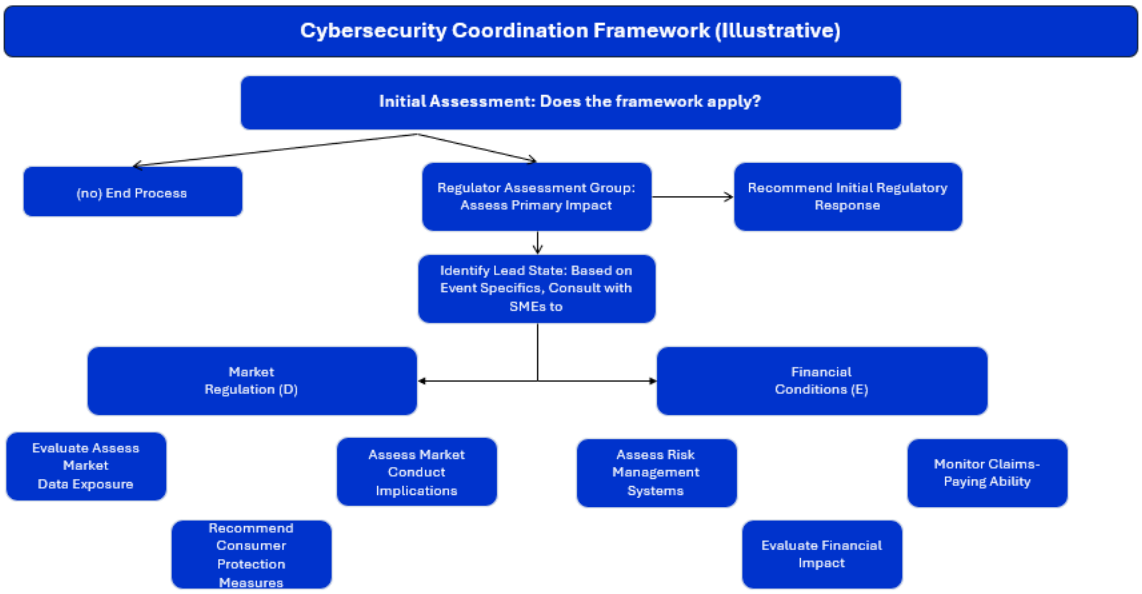
4. Coordinating Lead State Responsibilities

The Coordinating Lead State (Lead State) has the overall responsibility of facilitating communication and coordinating activities in an efficient manner. The Lead State is the key contact with the regulated entity under review. In coordination with the Cybersecurity (H) Working Group and other groups as appropriate, Lead State duties include:

- Convening the States for initial strategy planning to determine the appropriate course of action and scope of issues to be addressed.
- Prior to each NAIC national meeting and following any material event, providing status updates on the coordinated state response and on the cybersecurity event.
- Scheduling regular meetings and conference calls with the regulated entity to ensure that the process continues to be efficient and effective, and notifying the participating states as appropriate.
- As requested by any participating state the Lead State will work with NAIC staff to schedule conference calls. Calls will be open to all participating states where the current status of the cybersecurity event and coordinated response will be described, and any documents shared. All participating states will have an opportunity to ask questions.
- Determining if violations occurred and the extent of any violations found.
- Determining an appropriate corrective action by the regulated entity to ensure that further similar violations are prevented.

- Determining if a plan of remediation is necessary and its scope.
- Determining whether any post-action reporting by the regulated entity is needed.
- Determining the scope of post-action monitoring necessary by the Lead State.

5. Cybersecurity Coordination Framework – Illustrative



6. Relationship to other documents and projects

This Framework operates within a larger context that includes other NAIC documents, laws, and regulations. However, there are three documents/projects which play a more central role relative to responding to cybersecurity events. These are:

- The Cybersecurity Event Response Plan which is a resource that assists states responding to cybersecurity events happening within their domestic insurers.
- The Cybersecurity Event Response Coordination Framework described throughout this document.
- The Cybersecurity Event Notification Portal which is a tool that supports all regulatory responses whether for larger, national events, or for events where coordination is not as pivotal.