Attachment 2
Cybersecurity Event Response Coordination Framework 10-20-2026

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 Condition~~s~~ (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~~ Framework ~~includes detailed responsibilities for each~~ describes the role each committee will take in providing oversight of the coordination process, coordination mechanisms for complex events that cross jurisdictional boundaries, and specific implementation recommendations to formalize these procedures. ~~–~~The ~~F~~framework is designed to drive coordination particularly for information gathering to both enhance regulatory responses and reduce duplicative requests to industry in the wake of cybersecurity events.

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.

Relationship to the Cybersecurity Event Response Plan

The Cybersecurity Event Response Plan (CERP) is a foundational resource that may be utilized for cybersecurity event response. A department of insurance (DOI) that receives notification under Section 6 of the NAIC Insurance Data Security Model Law (#668), (hereinafter referred to as Model #668) or that otherwise becomes aware of a cybersecurity event at a regulated entity, may consult the CERP in navigating the DOI's response. In

© 2026 National Association of Insurance Commissioners

DRAFT

practice, a DOI may follow a response plan specific to their state but for ease of reference, this document will refer to the CERP.

This Framework builds on the CERP by adding a framework for coordination for the limited subset of events that warrant a coordinated multistate regulatory response.

What This Framework Does Not Do

Application of this Framework:

- does not expand the information a licensee is required to report beyond that described in Section 6(B), absent an examination or investigation brought under Section 7 of Model #668 or under other applicable state authority;
- does not confer on the NAIC, or on any state, authority that the state does not otherwise possess; and
- does not alter any state's confidentiality obligations or any licensee's ability to assert privilege or trade secret protection.

Where this Framework is applied, participating states will work to coordinate communication with the affected entity through the Coordinating Lead State. The reduction of duplicative regulatory requests is both a purpose of this Framework and a commitment of the states participating in it.

2. Evaluation and Response Process

As cybersecurity events take place, the Cybersecurity (H) Working Group (CWG) (hereinafter referred to as the CWG) will evaluate events and will engage with domestic regulators to see if the events would benefit from a coordinated response.

Generally, this Framework, and thus NAIC support, would apply to events that potentially affect policyholders across 5 or more states.

The evaluation of whether an event would benefit from the use of the Framework to guide coordination will also include consideration of the following criteria:

- The number of states in which consumers, policyholders, or operations are affected.
- The number of licensees affected by a common underlying event, including an event originating at a third-party or affiliated service provider or other shared technology dependency.

© 2026 National Association of Insurance Commissioners

DRAFT

- Operational impact to the affected licensee or licensees, including any impairment of claims handling, premiums processing, provider payment, or the ability to communicate with policyholders
- 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 cases where a singular event affects multiple entities)
- Operational impact ~~to~~to the company affected
- Whether the company operates internationally and if so, how international regulators are responding

The criteria in this section govern the coordination of regulatory responses among states. They do not establish, modify, or inform any threshold for a licensee's obligation to notify a commissioner of a cybersecurity event.

Response Protocol

Ongoing Activity - Monitoring

Over the course of the year, ~~NAIC staff will work with~~ the Cybersecurity (H) Working Group (CWG) will work with~~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. Such information gathering should take place within 30 business days of the identification of an event and rely on public information as much as possible.

Commented [LS1]: NAMIC recommends striking "NAIC staff" from the document where it relates to staff providing substantive assistance. The appropriate coordinating parties for carrying out the substance this Framework are the Cybersecurity Working Group and applicable Regulators only.

Paths to Consideration

An event may come before the Working Group for consideration under this Framework by any of the following paths, each of which is independent of the others:

1. Referral by the domiciliary regulator, or by a state previously identified as Lead State, under the CERP.
2. Request by any other state in which the affected licensee is licensed or operating, including any state that receives notification under a provision comparable to Section 6(A)(2) of Model #668.
3. Recommendation of the CWG leadership.

Step 1. Event Identification / Recommendation

© 2026 National Association of Insurance Commissioners

DRAFT

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

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

~~I.~~ Document a recommendation as to whether the Framework should apply for a given incident and refer the matter to MAWG.~~.~~

Commented [LS2]: NAMIC is suggesting the deletion of the NAIC staff reference, consistent with our earlier comment to this effect.

Commented [LS3]: Because the Framework contemplates using state statute via a lead state to protect information, data, and communication as a result of insurer inquiry (and the framework mimics the referral process already in place), NAMIC suggests the ultimate multi-state engagement be housed under MAWG.

~~II.~~ 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.

I.

II. The recommendation will also identify the presumed Coordinating Lead State and, where an alternate is proposed, the basis for the proposal.

~~a.~~

Step 2. Initial Communication

~~2.~~ Communicate the recommendation to the leadership of the:

~~a.~~I. Market Regulation and Consumer Affairs (D) Committee
~~b.~~II. Financial Condition (E) Committee
~~c.~~III. Innovation, Cybersecurity, and Technology (H) Committee
~~d.~~IV. Other Committee leadership as appropriate

Step 3. Activation and Lead State Identification

Based on responses received, applicable regualtors~~NAIC staff~~ and CWG leadership will identify a coordinating lead state as described in Section 3 of the Framework.

Commented [LS4]: NAMIC is suggesting deletion of the NAIC staff reference here, consistent with our earlier comment to this effect.

Step 4. Operation of the Framework

~~3.~~ ~~and work~~The Lead State utilizing~~via~~ the MAWG working group and structure ~~,~~ ~~with~~ support from the Cybersecurity (H) Working Group ~~and NAIC staff~~MAWG will work together under the appropriate state authority to facilitate coordinated inquiries of the affected company and facilitate information sharing, as appropriate, on the following:

Commented [LS5]: NAMIC suggests these changes, consistent with our comment directly above regarding MAWG referral.

I. Operational
   a. Status of resolution for any remediation of operational impacts including:
      i. ~~m~~Monitoring claims-paying ability
      ii. Ability to receive and process premium payments

© 2026 National Association of Insurance Commissioners

DRAFT

iii. Ability for policyholders to access coverage information

~~a.II.~~ Market Conduct
- ~~i.~~a. Examining consumer data exposure and notification requirements
- ~~ii.~~b. Assessing market conduct implications
- ~~iii.~~c. Reviewing compliance with privacy regulations
- ~~iv.~~d. Coordinating multi-state market conduct examinations
- ~~v.~~e. Monitoring consumer complaint patterns
- ~~vi.~~f. Evaluating producer licensing impacts
- ~~vii.~~g. Developing consumer protection measures

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

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

The ~~coordinating l~~Lead ~~state~~ State utilizing the MAWG working group and structure will work with ~~NAIC staff~~ and CWG leadership to provide communication via:

- ~~All state calls~~ Calls with all states / calls among affected states
- Regulator briefings
- 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

Commented [LS6]: NAMIC is suggesting removal of the reference to NAIC staff here, consistent with our earlier comment to this effect.

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~~ regulatory responses ~~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

© 2026 National Association of Insurance Commissioners

DRAFT

in a cybersecurity event response. The Lead State ~~is leading~~leads the state insurance regulatory response ~~primarily consisting of~~ with information gathering and dissemination of such information.

Presumption

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.

The domiciliary regulator, or a state previously identified as Lead State under those protocols, is presumed to serve as Coordinating Lead State under this Framework.

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 the 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~~ Lead ~~state~~State

Because each company or group has its own unique characteristics and similarly 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.

While Lead State selection will consider the adoption of the Model Law, it will not preclude the selection of non-adopting states as Lead States or from participating if states are able to ensure the confidentiality of information gathered in operating the Framework.

As the NAIC deploys this framework, after action meetings may take place allowing lessons learned to inform future revisions to the Framework.

© 2026 National Association of Insurance Commissioners

DRAFT

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 sStates for initial strategy planning to determine the appropriate course of action and scope of issues to be addressed.
- Requesting that participating states work to gather information jointly, as appropriate.
- 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.
- Working with participating states to ensure information shared is properly held confidential, as appropriate.
- Determining, in conjunction with participating states, if violations occurred and the extent of any violations found.
- Determining and coordinating an appropriate corrective action by the regulated entity to ensure that further similar violations are prevented.
- Determining, in conjunction with participating states, 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.
- Determining, in conjunction participating states, when the coordination process and related inquiry should be concluded.
- Serving as the single point of contact for the affected entity, and receiving notice of any information request a participating state proposes to make outside the coordinated process.
- Maintaining the shared record of the coordinated response in the environments described under Section 6 “Confidentiality” below.

© 2026 National Association of Insurance Commissioners

DRAFT

Working through the Lead State to request information, the Framework should assist in reducing duplicative requests allowing states to gather information jointly.

Participating State Responsibilities

A state participating in a coordinated response under this Framework:

- Executes the information sharing and confidentiality agreement described under "Confidentiality" below, or identifies the limits its own law places on its participation;
- Directs information requests to the affected entity through the Coordinating Lead State, and gives the Coordinating Lead State notice of any request it must make independently;
- Shares with participating states, to the extent its own law permits, information it receives regarding the event;
- Identifies a point of contact for the duration of the coordinated response; and
- Maintains shared information consistent with its own confidentiality obligations and with the terms of the agreement.

Participation is voluntary. A state may participate in a coordinated response without ~~relinquished~~relinquishing any authority, and may decline to participate without prejudice to any action it takes independently.

5. NAIC Support Responsibilities

The support that NAIC provides may vary from event to event depending on state needs. However, NAIC staff may be asked to:

- Assist in gathering and reviewing publicly available information on a cybersecurity event.
- Assist in the logistics of coordination calls including scheduling and provisioning of meeting notices.
- ~~Advising state insurance regulators on technical subject matters relating to the Information Data Security Model Law or examination authority.~~
- Limited review and assessment of technical information intended to support state cybersecurity event responses.

Formatted: Indent: Left: 0.5", Hanging: 0.08", No bullets or numbering

Commented [LS7]: NAMIC suggests deletion of this bullet point, as it is not appropriate for NAIC staff to be advising on substance relative to Model 668 or exam authority.

DRAFT

© 2026 National Association of Insurance Commissioners

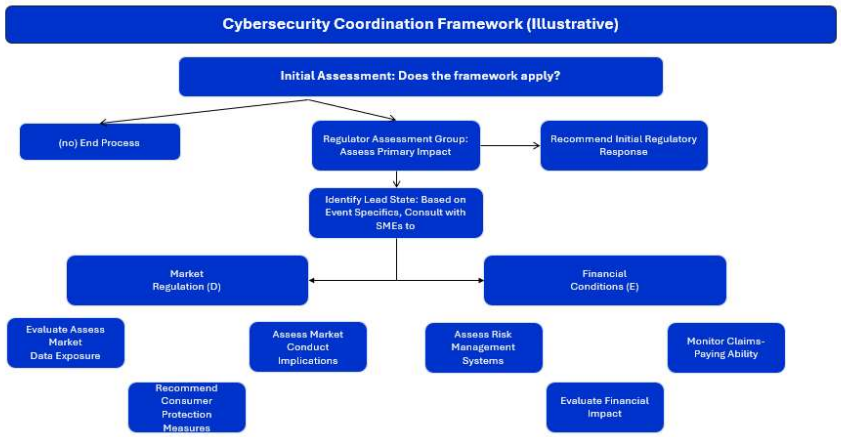
6. Confidentiality

As states are requesting information, states will ensure confidentiality of information specific to each situation. States will generally rely on the authority afforded to states via their implementation of either the Model Law #668 and the authority to investigate cybersecurity events it provides, or the state examination authority.

Confidentiality will depend on the states involved and on the information being gathered. Information on how each Lead State will provide confidentiality for requested information will be addressed on a ~~case by case~~case-by-case basis.

7. Cybersecurity Coordination Framework in Operation – ~~Illustrative~~Illustrations

~~5.~~ To assist in explaining the operation of the Framework, the following illustrations were created depicting key concepts.



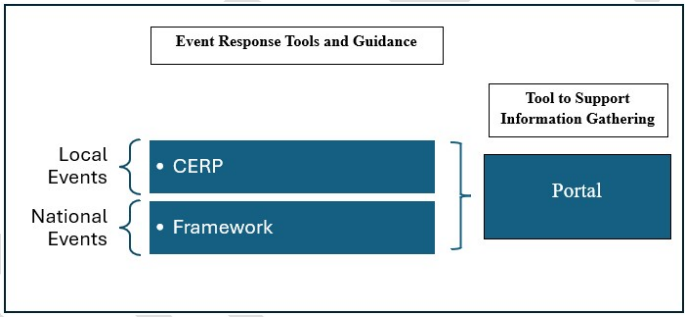
© 2026 National Association of Insurance Commissioners

© 2026 National Association of Insurance Commissioners

~~6.~~8. 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~~ affecting 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.



© 2026 National Association of Insurance Commissioners

© 2026 National Association of Insurance Commissioners

Attachment 2
NAIC Summary of Framework Comments 10-20-2026

Comment Summary and Summary of Changes

To assist stakeholders in understanding the changes to the latest version of the Cybersecurity Coordination Framework, NAIC staff have prepared this summary with notations for how the Framework has been updated to reflect the input received.

Who commented

- **Information Technology Examination (E) Working Group**
- **NAMIC**
- **California DOI**
- **New York DFS**
- **ACLI**
- **AHIP**
- **APCIA**
- **BCBSA**

Key themes and how the revision responds

1. Support for coordinating, with a narrow scope. Nearly every commenter backed the lead-state idea as a way to cut duplicate requests. Stakeholders expressed input ranging from support for the idea without material changes to workable to expressing caution against creating a "51st state" or a central supervisory layer.

- *Revision:* A new "What This Framework Does Not Do" section says the Framework adds no reporting duties, gives no state or NAIC new authority, and changes no confidentiality or privilege protections.

2. Activation criteria and scope. Stakeholders said the catch-all clause left no real threshold with some asking for objective criteria based on material impact. Other stakeholders asked about the Framework's purpose and intended uses.

- *Revision:* The catch-all clause is gone. The Framework now generally applies to events that may affect policyholders in 5 or more states, with clearer factors to weigh.

3. Confidentiality and information sharing. Several stakeholders raised concerns about how sensitive information would be protected as it moves between states and NAIC staff.

- *Revision:* Additional language on confidentiality has been added.

© 2026 National Association of Insurance Commissioners

4. Portal access and states without Model #668. Several stakeholders all raised the problem that the Portal is limited to states that adopted Model #668 and to whether a lead state that hasn't adopted Model #668 would be disqualified.

- *Revision:* Not adopting Model #668 doesn't automatically stop a state from leading or participating, as long as it can keep information confidential. Additional text distinguishing the Portal as a tool from the Framework as a process of coordination was added. The edits further add that there are many ways that a Department of Insurance may learn about an event.

5. Choosing the lead state and its role. Stakeholders posed numerous questions about lead state selection with several also suggesting a default rule. Stakeholders also suggested that the lead state function as the main point of contact in discussions with the affected insurance company.

- *Revision:* The domiciliary regulator, or an existing lead state, is presumed to lead. Participating states will route communication through the lead state.

7. NAIC staff role. Stakeholders asked for more clarity on the NAIC's role in this framework.

- *Revision:* A new section describes NAIC staff's supporting role has been added.

8. Clarity of the Process. Stakeholders offered input that the actual process of coordination was unclear.

- Revision: Several edits aimed at clarifying the progression of coordination were added.

© 2026 National Association of Insurance Commissioners

© 2026 National Association of Insurance Commissioners