November 19, 2026
Via email: pwallace@naic.org

Brett Bache, Chair
Danielle Torres, Vice Chair
Market Conduct Examination Guidelines (D) Working Group
National Association of Insurance Commissioners

Re: Revised Cybersecurity Event Response Coordination Framework (October 20, 2026 Draft)

Dear Chair Bache, Vice Chair Torres, and Members of the Working Group:

Pinpoint Policy Institute ("PPI") appreciates the opportunity to comment on the October 20, 2026, revised draft of the Market Conduct Examination Guidelines (D) Working Group's ("Working Group") **Cybersecurity Event Response Coordination Framework ("Framework")**.[1]

PPI supports the Framework's core goal and timely work. When one cyber event reaches insurers and policyholders in many states, regulators should act together, and companies should answer one set of questions instead of dozens. The revised Framework makes real progress toward its intended outcome of fewer duplicate requests without establishing new or expanded reporting requirements or examination and supervisory authorities. It adopts a five-state threshold, makes the domestic regulator the presumed Lead State, defines the NAIC staff role, and adds a section explicitly outlining what the Framework does not do.[2] Those changes answer many concerns raised against the initial Framework exposure.

PPI recommends that the Working Group address three remaining gaps before adoption. Our specific comments follow.

1. The Lead State's Role Should Stay Coordination, Not Enforcement.

The new "What This Framework Does Not Do" section states that the Framework grants no state or the NAIC any new authority.[3] Section 4 then assigns the Lead State, with participating states, responsibility for determining whether violations occurred, the extent of violations, corrective action, remediation plans, post-action reporting, and the scope of post-action monitoring.[4] Section 2 adds coordinating multistate market conduct examinations and determining potential rating implications.[5]

These are enforcement and supervisory functions, causing the language to sit uneasily with the Framework's statement that it confers no authority a state does not already have. A Lead State has no

[1]NAIC, Cybersecurity Event Response Coordination Framework, Attachment 2 (draft dated Oct. 20, 2026) [hereinafter "Framework"].
[2]NAIC, Summary of Framework Comments (Oct. 20, 2026) [hereinafter "Comment Summary"].
[3]Framework, supra note 1, § 1.
[4]NAIC, Cybersecurity Event Response Coordination Framework, Attachment 2 (draft dated Oct. 20, 2026), § 4.
[5]NAIC, Cybersecurity Event Response Coordination Framework, Attachment 2 (draft dated Oct. 20, 2026), § 2 (Step 4).

© 2026 National Association of Insurance Commissioners

jurisdiction to find that a company violated another state's law or to impose remedies on a company domiciled elsewhere.

First round commenters warned against a "51st state" and against states using shared incident data to open exams they could not otherwise open.[6] The new section addresses that concern in principle; Section 4 reopens it in practice. The Working Group should limit the Lead State's role to collecting and distributing information. Findings of violation and any remedies should remain with each state that has jurisdiction and should follow that state's existing exam and due process rules. Post-event monitoring should have a defined scope and an end date.

2. Affected Companies Need a Defined Role and Privileges.

The draft Framework gives the company no notice when the Framework is activated, no input on Lead State selection, and no chance to correct facts before regulators brief one another. The Lead State would also prepare talking points for outside inquiries about the event.

Regulator statements made without the company's input could conflict with its required disclosures, including SEC filings, consumer notices, and law enforcement requests to delay disclosure. Inaccurate public statements could also mislead policyholders.

The Framework should require prompt written notice to the company when the Framework is activated and when a Lead State is named. It should also give the company a chance to review factual statements before they are shared outside the participating states and require coordination with law enforcement before any public statement.

In the first days of an attack, the company's response team must focus on containment, restoring service, and protecting policyholders. The Framework's process lacks deadlines for Steps 1 through 3.[7] The NAIC knows from its own incident that early facts are incomplete; its forensic review ran for weeks with limited public updates.[8] Insurers deserve the same room.

PPI recommends that Working Group set clear target timelines for Steps 1 through 3, and limit initial regulator contact to one Lead State call that pertains only to policyholder-facing operations such as claims payment, premium processing, and access to coverage information. Formal information requests as outlined in the Framework would follow.

3. Confidentiality Protections Must Be Defined Before Information Is Pooled.

The Framework would collect sensitive incident data from an insurer during or shortly after an attack and share it among many states. In response to stakeholder comments regarding data confidentiality, the Working Group included "additional language" addressing the topic in the revised Framework.[9] These additions remain insufficient.

Section 6 of the Framework states that confidentiality decisions will be addressed case by case. Section 4 refers to an "information sharing and confidentiality agreement" and to shared record "environments" described in Section 6; Section 6 describes neither.[10]

[6]ACLI, Comments on the Cybersecurity Event Response Coordination Framework (July 24, 2026); APCIA, Comments on the Cybersecurity Event Response Coordination Framework (July 24, 2026).
[7]Framework, supra note 1, § 2.
[8]Security Update, supra note 5.
[9]Comment Summary, supra note 2, at 1.
[10]NAIC, Cybersecurity Event Response Coordination Framework, Attachment 2 (draft dated Oct. 20, 2026), §§ 4, 6.

© 2026 National Association of Insurance Commissioners

The draft also allows states that have not adopted Model #668 to lead or participate if they can "ensure the confidentiality" of shared information, but it sets no standard for that showing.[11] A company should not learn the rules for protecting its forensic findings after it has already produced them.

Pooled incident data itself is an attractive target and no organization is invulnerable to attack, as demonstrated earlier this year, when the NAIC disclosed that unauthorized parties accessed its systems and took and published confidential regulatory data. A consolidated record of an insurer's vulnerabilities, compromised systems, and remediation status could cause serious harm if exposed. The Framework should set binding safeguards before any information moves, including:

- a model confidentiality agreement, attached to the Framework, that each participating state signs before receiving information;
- a minimum showing for states without Model #668 confidentiality protections;
- data minimization, access controls, retention and deletion schedules, and limits on further disclosure;
- security standards for the shared record environment and a duty to notify the company if regulator held data is compromised; and
- an express statement that sharing privileged material among participating states does not waive privilege or work product protection, supported by common interest treatment where state law allows.

Additional Points.

Several commenters asked for objective, impact-based activation criteria.[12] We note that a five-state count alone, as included in the revised Framework, will capture nearly any event at a national carrier. PPI recommends adding a materiality test tied to policyholder harm, so that the Framework applies by exception rather than by default.

Cyber events at insurers involve many authorities besides insurance regulators, including federal cybersecurity agencies, law enforcement, the SEC, state attorneys general, and other state regulators.

The Framework should commit the Lead State to coordinate with these authorities where feasible, accept reports already filed with them where they meet regulators' needs, and defer to law enforcement requests concerning timing and disclosure.

[11]NAIC, Cybersecurity Event Response Coordination Framework, Attachment 2 (draft dated Oct. 20, 2026), § 3.
[12]Comment Summary, supra note 2, at 1.

© 2026 National Association of Insurance Commissioners

Conclusion.

PPI respectfully asks the Working Group to make these changes and re-expose the revised Framework for comment. Coordination will work only if companies can trust that their information is protected and that the Framework's limits mean what they say.

Sincerely,

Eric Ventimiglia

Eric Ventimiglia
Executive Director
Pinpoint Policy Institute

© 2026 National Association of Insurance Commissioners