Draft: 03/18/26

Cybersecurity (H) Working Group
Virtual Meeting
March 13, 2026

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met March 13, 2026. The following Working Group members participated: Michael Peterson, Chair (VA); Colton Schulz, Vice Chair (ND); Alex Romero and Molly Nollette (AK); Mark Fowler and Richard Fiore (AL); Lori Dreaver Munn (AZ); Wanchin Chou (CT); Tim Li (DE); Matt Kilgallen (GA); Daniel Mathis (IA); C.J. Metcalf (IL); Shane Mead (KS); Kallie Ruggiero Somme (LA); Dmitriy Valekha (MD); Danielle Torres (MI); Gregory Maus (MN); Kim Dobbs (MO); Martin Swanson (NE); Joshua Hilliard (NH); Roger Hayashi (NV); Gille Ann Rabbin (NY); Matt Walsh (OH); Sebastian Conforto (PA); Jamie Adams (WI). Also participating was: Matthew Gendron (RI).

1. Discussed Proposed Edits to the Cybersecurity Event Notification Portal Project Intake Form

Peterson presented a brief summary of the proposed changes made in response to the most recent public exposure period. He noted the inclusion of the first draft of the standard form through which licensees will report cybersecurity event notifications in the portal. Peterson reiterated there is no intention to charge licensees to use the portal. Additional language was added to clarify the System and Organization Controls (SOC) 3 report as requested by industry stakeholders. He reminded the Working Group that SOC exams are performed by licensed Certified Public Accountant (CPA) firms operating under the American Institute of Certified Public Accountants (AICPA) attestation standards

Peterson suggested the next steps for the portal project would be to get the document adopted and, then begin the design and development of the portal through consultation and discussion with stakeholders. The first step in ensuring the portal operates correctly is for regulators to draft the standard form based on Section 6B of the Insurance Data Security Model Law (#668). Peterson said once the NAIC has completed enough development, testing will begin with regulators to ensure it is working correctly. He described that the governance and security procedures could be tested through tabletop exercises using synthetic data to simulate various event types and illustrate the different controls and functions that ensure data is protected. He said that the next steps would require substantial engagement with stakeholders, the industry and regulators, to ensure the portal is developed to deliver the expected functionality, usability, and reduction in complexity

2. Adopted the Centralized Cybersecurity Event Notification Portal Project Document

Dobbs provided a summary of the change management process and explained that many of the comments focused on details such as user access, which is typically provided in different technical requirements documents associated with later parts of the process. She explained that the industry would be invited to provide feedback and participate in collaborative discussions and testing.

Schulz highlighted that, although there is limited direct overlap between the groups, the drafting group for the *Market Conduct Exam Handbook* has begun developing a national response framework for cybersecurity events affecting multiple jurisdictions and entities. He noted that this work assumes the existence of shared reporting and coordination functionality similar to what is being discussed for the portal and encouraged the Working Group to remain mindful of other related workstreams that may touch on or benefit from these capabilities.

Holly Weatherford (Wholesale and Specialty Insurance Association—WSIA) thanked the Working Group for the revised project proposal and expressed appreciation for the collaborative engagement. She stated that the WSIA supports the concept of a licensee-directed cybersecurity event notification portal and recognizes that the revisions reflect movement toward that model. She raised concerns, however, that certain proposal language regarding regulator access could be interpreted to allow broader regulatory discretion. Specifically references to departments being "legally entitled" to access notifications could raise concerns about data governance and legal boundaries. She requested additional clarity and transparency on the intent, scope, and limits of regulator access, and on how access would be structured to align with state law while preserving the licensee-directed framework. She also acknowledged revisions emphasizing reduced compliance costs, noted the removal of references to portal fees and revenue concepts, and asked for ongoing transparency on costs and any future revenue considerations.

Lindsey Stephani (National Association of Mutual Insurance Companies—NAMIC) stated that NAMIC submitted comments and redlines consistent with themes raised throughout the project and thanked leadership for ongoing engagement and discussion. She requested that the meeting minutes reflect that the discussion of the depth and sensitivity of information to be collected will occur later, potentially as part of future technical document discussions. She explained that this request is driven by concerns about concentration risk and concluded her remarks.

Peterson thanked Ms. Stephani and acknowledged her interests and stated there will be multiple future opportunities to discuss those topics. He emphasized that there is no intention to move forward unilaterally or predetermine outcomes, and that questions regarding both the substance and implementation will be addressed as they arise.

LaCosta Wix (AHIP) thanked the Working Group for the opportunity to comment on the recent iteration of the centralized portal intake request form and expressed appreciation for the goal of reducing administrative friction for plans experiencing reportable cybersecurity events. She acknowledged the work completed to date and noted that her organization submitted written comments with more detailed questions and requests for clarification, some of which may be addressed in the revised draft. She emphasized the importance of ensuring robust security and confidentiality protections for the portal given the sensitivity of the information it will house and concluded by thanking the Working Group for the opportunity to comment.

Peterson thanked AHIP and stated that the Working Group appeared aligned and prepared to begin work on the project, with the understanding that outstanding questions and concerns raised in comments would continue to be addressed as the work progresses. He noted his intent to keep those issues in view and work toward resolving the most important items as the project moves forward.

Peterson made a motion, seconded by Dobbs, to adopt the revised centralized cybersecurity event notification portal project document (Attachment XX) as exposed.

The motion passed unanimously.

Having no further business, the Cybersecurity (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2026_Spring/WG-Cybersecurity/2026 0313Interim-Meeting/Minutes-CyberWG031326.docx

Draft: 12/17/25

Cybersecurity (H) Working Group
Hollywood, Florida
December 10, 2025

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Hollywood, FL, Dec. 10, 2025. The following Working Group members participated: Michael Peterson, Chair (VA); Colton Schulz, Vice Chair (ND); Julia Jette (AK); Mark Fowler and Richard Fiore (AL); Chris Erwin (AR); Lori Dreaver Munn (AZ); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Elizabeth Nunes and Matt Kilgallen (GA); Kathleen Nakasone (HI); Daniel Mathis (IA); Ryan Gillespie (IL); Eric Turek and Shane Mead (KS); Dominique Jones (LA); Danielle Torres (MI); Kim Dobbs (MO); Gregory Maus (MN); Jacqueline Obusek (NC); Joshua Hilliard and Christian Citarella (NH); Roger Hayashi (NV); Gille Ann Rabbin (NY); Matt Walsh (OH); David Buono (PA); Todd Lovshin (WA); Rebecca Rebholz and Christina Keeley (WI); and Lela D. Ladd (WY).

1. Adopted its Sep. 25 Minutes

The Working Group met Sept. 25 and took the following action: 1) adopted its Summer National Meeting minutes; and 2) adopted the IDSM Compliance Guide and Chief Financial Regulator Forum response.

Mathis made a motion, seconded by Torres, to adopt the Working Group's Sept. 25 (Attachment Three-A) and Summer National Meeting minutes (*see NAIC Proceedings – Summer 2025, Innovation, Cybersecurity, and Technology (H) Committee*). The motion passed unanimously.

2. Discussed the Cybersecurity Event Notification Portal and Heard Comments from Interested Parties

Peterson provided an overview on the Working Group's progress toward achieving convergence in implementation and operation of the *Insurance Data Security Model Law* (#668). Two major work products completed so far are the Cybersecurity Event Response Plan and the IDSM Compliance Enforcement Guide. These tools are designed to align states responses and enforcement practices under Model #668, reducing regulatory complexity and marginal costs for industry. He explained that the portal is intended to streamline cybersecurity event notifications, reducing administrative burden and marginal costs for insurers operating in multiple states. Petersons described how Section 4 and Section 5 of Model #668 impose low marginal costs, but Section 6 and Section 7 create significant challenges, which the portal aims to address.

Peterson explained that following the Working Group's motion for the NAIC to explore the development of the portal at the 2024 Fall National Meeting, the project management office has implemented a new process in order to ensure as much buy in and support as possible. He described the portal being planned as a modest, push system, where a licensee experiencing a cybersecurity event would select the states for which they want to send their notifications. The system would only allow state insurance regulators from states selected to view any information submitted in the form.

Ladd and Peterson discussed the limitation of the portal to only those states that have adopted Model #668, the idea being the data security law affects insurance specifically. Opening the portal to other agencies would be a long and challenging process.

Torres suggested the portal could be helpful for companies and state insurance regulators. She emphasized that it must be a secure option that allows for correspondence between the states and the insurers, to ensure that all necessary information is available.

Kirsten Wolfford (American Counsel of Life Insurers—ACLI) encouraged further adoption of Model #668 and uniformity across the insurance jurisdictions. She also stressed the importance of confidentiality and security of the portal.

Kristin Abbott (American Property Casualty Insurance Association—APCIA) supported the centralized portal concept and requested opportunities for feedback on prototypes and operational details as the project develops.

John Meetz (Wholesale and Specialty Insurance Association—WSIA) whose submitted comments were joined by the Council of Insurance Agents and Brokers (CIAB) agreed with the previous comments and raised questions about reconciling varying state notification requirements. Meetz and Peterson discussed regulatory access to the portal as role-based access granted only to the states included in the notification selections made by the licensee's submitting.

Lindsey Stephani (National Association of Mutual Insurance Companies—NAMIC) expressed support for improving efficiency in cybersecurity event reporting, noting that inconsistent requirements across states and agencies create significant burdens and divert resources from incident response. However, NAMIC raised concerns about the level of sensitive information that would be centralized in the proposed portal, particularly if detailed data were required. Stephani requested that the Working Group clarify and document expectations regarding data granularity in the project proposal to help address these concerns. NAMIC reiterated its appreciation for the opportunity to provide input and referenced its extensive written comments submitted for consideration.

Peterson and Miguel Romero (NAIC) presented and discussed options for the Working Group to consider as the appropriate next steps for the project's advancement. The Working Group's members suggested the document be updated to provide additional details to address the concerns raised.

Munn suggested making corrections and revisions to the portal documentation first, to allow an opportunity for other concerns to be raised by members and interested parties of the Working Group.

Schulz shared that North Dakota implemented a SharePoint-based notification system about three years ago, which took only a few hours to build and functions similarly to the proposed portal. This system improved security and access control compared to the previously used shared email method, which was relatively unsecure. Schulz emphasized that most states still rely on email for notifications and stated that moving to the proposed portal would be significantly more secure. He recommended building the portal now and allowing state insurance regulators to use it and provide feedback.

Mathis and Peterson emphasized that security and confidentiality were top priorities for both state insurance regulators and industry stakeholders. Suggestions included adding more detail in project documentation about security measures to reassure participants and committing them to demonstrate compliance with recognized standards (e.g., SOC 3) on an ongoing basis, rather than simply stating intent. Regulators also noted that data governance and access control, ensuring that only regulators with legal authority can view notifications, must be clearly implemented and verifiable. The Working Group agreed that these assurances can best be demonstrated once the portal is built, but the intent to include robust review and security validation should be documented.

Stephani reiterated concerns about the portal project intake form specifying all aspects of Section 6B of Model #668, particularly Subsection 10 and Subsection 11, which could require highly detailed and sensitive information. NAMIC requested that the Working Group clarify its intent and document that submissions should remain high-level to avoid centralizing excessive sensitive data. Peterson responded that, in practice, Section 6B questions typically require brief, basic reporting rather than detailed disclosures, and additional information can be requested directly if needed. The Working Group discussed whether to revise the intake form to reflect this clarification before adoption or proceed with the current version and address concerns during implementation.

Dobbs clarified that the current document under discussion serves as a high-level project proposal to determine whether the portal should be pursued, rather than a technical specification. She noted that detailed elements, such as specific questions, user access levels, and other operational details, would typically be addressed later in a technical proposal after the decision to proceed with the project.

Romero noted that revisions to clarify intent could be made without significantly delaying the project but emphasized that the decision ultimately comes down to whether the Working Group wants to adopt the document as-is or request revisions before proceeding. The Working Group acknowledged that the complexity of revisions could vary and would become clear once proposed edits are reviewed

The Working Group decided to revise the form based on input received.

3. Heard a Presentation on the 2025 Cybersecurity Insurance Report

Chou provided highlights from the 2025 Cyber Insurance Report, noting that the cyber supplement was revised in 2024 to integrate primary, excess, and surplus lines reporting. He shared that the global cyber insurance market reached approximately $15 billion in 2024, with the U.S. representing the majority of business and growth emerging in Asia and other regions. Chou observed underwriting cycle trends, including a decline in ransomware incidents in recent years and the emergence of new attack types such as “Scattered Spider.” He emphasized that AI-driven threats underscore the continued importance of cyber insurance and encouraged members to review the report prepared by the NAIC for further discussion.

Henry presented key findings from the 2025 Cyber Insurance Report, noting that after slowed growth in 2023, the U.S. cyber insurance market declined for the first time in 2024 by approximately 7.11% (or 2.3% excluding alien surplus lines). He highlighted that 65% of policies were written as primary, while excess and endorsement policies represented a smaller share of premium volume. Henry suggested exploring alternative metrics, such as direct written premium compared to loss ratios, in future reports to provide more meaningful insights. He invited state insurance regulators to collaborate on the 2026 report to make it more actionable and useful, encouraging feedback on additional data points to include.

Romero emphasized the importance of ensuring that the annual cyber insurance report is useful and actionable for state insurance regulators and industry stakeholders. He encouraged feedback on whether the current data presentation meets market intelligence needs and invited suggestions for improving how information is compiled and displayed. Romero stressed that input from the community is essential to make the report more valuable for state insurance regulatory oversight and market analysis, and urged members to review the content and share ideas for enhancements

Having no further discussion, the Cybersecurity (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2025_Fall/WG-Cybersecurity/Fall-Minutes/Minutes-CyberWG-121025-Draft.docx

