

# 1. Consider Adoption of its Oct. 30 Minutes

## Attachment A

*–Cynthia Amann (MO)*

Draft: 11/16/24

Cybersecurity (H) Working Group  
Virtual Meeting  
October 30, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met Oct. 30, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Julia Jette (AK); Leo Liu (AR); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Matt Kilgallen (GA); Lance Hirano (HI); Daniel Mathis (IA); C.J. Metcalf (IL); Shane Mead (KS); Mary Kwei (MD); Jeff Hayden (MI); Bubba Aguirre (MN); Troy Smith (MT); Tracy Biehn (NC); Colton Schulz (ND); Christian Citarella (NH); Scott Kipper (NV); Gille Ann Rabbin (NY); Don Layson (OH); David Buono (PA); John Haworth (WA); Andrea Davenport (WI); and Lela Ladd (WY).

1. Adopted Its Oct. 8 Minutes

The Working Group met Oct. 8 and took the following action: 1) heard an informational presentation from the Federal Bureau of Investigation (FBI) Internet Crime Complaint Center (IC3) on its programs, the cyber risk and threat landscape, reporting, and incident handling resources.

Schulz made a motion, seconded by Buono, to adopt the Working Group's Oct. 8 minutes (Attachment XX). The motion passed unanimously.

2. Heard an Update on the Progression of the CERP and the Model #668 Survey

Peterson initiated the conversation with a reminder of the passing of the Cybersecurity Event Response Plan (CERP) and the subsequent discussions about exploring a centralized reporting system. After conversations with state insurance regulators, industry, and NAIC staff, Peterson suggested that the most logical approach would be to create an NAIC portal that would allow for cybersecurity event notifications to be submitted in a centralized way to reduce the reporting burden placed on companies. Peterson further described the seemingly avoidable complications of a system not built to accommodate future statutes and reporting legislation.

Peterson described the plan as having a two-pronged approach to address the repository security and access control concerns. The first is to create a minimally functional portal so the necessary testing of security and access controls can be conducted and reviewed. The second is to implement and manage the convergence of future reporting legislation. With the focus on compliance on the front end, achieving regulatory convergence later becomes simpler. The first narrowly scoped portal would include only the questions and statutory construction of the *Insurance Data Security Model Act* (668). Peterson explained that early and obvious improvements will be made to future versions to reflect the states with adopted legislation that varies from Model #668.

Peterson introduced the idea of using synthetic data generated from artificial intelligence (AI) to simulate different cybersecurity events. This was first mentioned by Allison Parent (Global Financial Markets Association—GFMA), an industry expert. Peterson proposed using tabletop exercises to demonstrate the portal's ability to adhere to confidentiality rules for all stakeholders. Concurrently with testing plans, he suggested a survey to states be conducted to better understand what individual implementations of Model #668 look like, as well as any specific differences between the model law and the language state legislature produced. Future improvements can be made as a result of the survey and regulatory convergence achieved without impacting the security, and access controls proved secure through the exercises.

Peterson proposed the creation of a motion to construct an NAIC portal, designed to be minimal, reflecting only the functionality of Section 6 of Model #668, with plans to improve overtime to reflect actual legislation. The portal will be used to test the applicable security and access controls to demonstrate that industry data is kept confidential, as required by Model #668. Concurrently with testing, a survey will be sent to states to understand requirements to bring the portal's design in synch with existing legislation. He described the Change Healthcare incident as a recent and relevant example of an incident for which a portal such as this would have recognizable benefits.

Peterson stated a second motion would be necessary after completing the work required within the adopted first motion. He said the focus would be on implementation and regulatory convergence. Peterson reminded the Working Group that immediate implementation of a minimal portal would greatly reduce the regulatory burden and simplify the cybersecurity event notification processes for all Model #668 states. The survey to states and the plan to perform future improvements to achieve regulatory convergence will be a project plan item.

In summary, Amann and Peterson said the two motions support a single project. They asked for comments and encouraged questions to be shared. They jointly encouraged a motion to be discussed and voted on at the Fall National Meeting.

Schulz asked whether the chairs foresaw a need for a drafting group to work on items related to the second motion. Peterson explained that the survey results would need to be reviewed by a group to be turned into a project plan or at least items of a plan.

Miguel Romero (NAIC) suggested a summary of the two motions for the project be distributed to the Working Group distribution list, requesting and encouraging all recipients to consider providing comments to be received before and during the Fall National Meeting.

Debra Decker (Stimson Center) inquired whether the project intended to consider federal harmonization efforts by other regulatory organizations. Peterson suggested future improvements could be discussed when appropriate, as the Working Group's efforts to create a centralized reporting repository are trending slightly ahead of federal organizations.

### 3. Heard a Presentation on the 2024 Cyber Insurance Report

Koty Henry (NAIC) introduced the 2024 Cyber Insurance Report. He explained that the sourced data is pulled from the NAIC's *Property/Casualty Annual Statement Cybersecurity and Identity Theft Supplement* (Cyber Supplement) and the alien surplus lines data from the International Insurers Department (IID). The Cyber Supplement requires U.S. domiciled insurers to report information on stand-alone cybersecurity insurance policies and coverage sold as part of a package policy. Henry stated the information reported includes but is not limited to the first- and third-party claims, direct premiums written and earned, and the number of policies in force.

Henry gave a market overview, stating that global premium reached \$16.66 billion for cyber coverage in 2023, and the U.S. cyber insurance market remains the largest with a 59% market share. Henry stated that the cyber threat landscape continues to break records as it becomes more volatile and complex, and global cyber insurance premiums are projected to exceed \$50 billion by 2030. The increasing number of cyber incidents is driving demand for appropriate coverage to mitigate financial losses. He further explained that small- and medium-sized enterprises (SMEs), a particularly vulnerable business sector, are expressing interest in cyber insurance, as companies in all revenue bands are targeted. An 11% increase in policies in force counts reflects a growing demand for cyber insurance coverage. Henry stressed the importance of maintaining good cyber hygiene practices and not allowing growth in the comfort and stability of the cyber insurance market to be viewed as an opportunity to

become complacent. Referring to 2023 claims data, Henry reported ransomware and business email compromise claims were trending up in frequency and severity. Companies earning more than \$100 million in revenue saw a 20% increase in the number of claims and a 72% increase in claims severity compared to the second half of 2022.

Henry explained that events like the July 2024 CrowdStrike incident demonstrate the need for cyber insurance at a time when 72% of SMEs without cyber insurance say a major cyberattack could destroy their business. Henry described how cybersecurity teams are turning their attention to proactive threat intelligence instead of reacting to threats once they become attacks. They use threat intelligence to increase visibility and mitigate risks to stay several steps ahead of threat actors. Insurers are focusing on managing systemic risk to limit aggregate exposures, some using active monitoring of policyholder system infrastructure to assist.

Henry then provided a list of the top three risks and threats, including a caveat to suggest the overview is not exhaustive and an hour-long presentation could not fit such a list. Henry introduced the term business email compromise (BEC) and explained that Coalition Incident Response (Coalition) reported phishing emails as the number one root cause for BEC claims in the first half of 2024. BEC claims accounted for nearly a third of all Coalition claims during the same period. Advancements in AI have been reflected in the improvement of phishing emails. Henry said threat actors who historically were known for poor grammar and typos have used AI to draft near-flawless emails. He explained that data breaches continue to greatly impact sectors such as healthcare and financial services due to the sensitive nature of the data they handle. Costs associated with data breaches usually include notification expenses, legal fees, regulatory fines, and credit monitoring services for impacted individuals. Henry suggested marketplaces such as the Silk Road and Tor2dor remain relevant concerns because the nature of the dark web, in which they reside, supports almost complete anonymity. Cyber threat actors use the dark web marketplaces to offer illicit digital goods and stolen identification information.

Henry said cyber insurance has evolved significantly, becoming a crucial component in the broader cybersecurity landscape. He said it provides a vital safety net for businesses, helping to mitigate financial losses from data breaches, ransomware campaigns, and business-related interruptions. In 2024, cyber insurance policies have increasingly incorporated language to address unplanned outages and provide contingent business interruption coverage. Henry said this shift in language aims to ensure recovery from disruptions that do not result from a cyberattack, such as those caused by non-malicious events like human error. He added that state insurance regulators continue to monitor and assess the market to better understand how the industry protects policyholders. The state insurance regulators seek to discuss and better understand considerations such as the availability, affordability, and pricing of cyber insurance products, disclosures, policy limits, underwriting practices, and the role of reinsurance in the cyber insurance market.

Henry said that, in conclusion, cyber threat actors and criminals are not waiting; therefore, a proactive approach to security is essential. Henry referred to a recent U.S. Department of Defense (DOD) report that an alarming 4% of defense contractors are in compliance with even the most basic cybersecurity requirements. Henry stated that the guiding doctrine was published almost a decade prior to the report and opined that self-attestation without regulatory oversight likely had a hand in so many companies reportedly being non-compliant. Henry said that some SMEs expected to be included in the growing trend of those seeking cyber insurance are part of the defense industry sector.

Chou asked if Henry could provide additional input on how state insurance regulators might be able to provide the necessary education or incentives to help increase the awareness of and take up rate for cyber insurance. Amann suggested that while it might be a complicated answer, state insurance regulators should step up the focus and discussion of cyber hygiene and cyber event prevention. Amann said there is still a need for good cyber practices, oversight, and continued education and that buying coverage is just the first step. She suggested

collecting and analyzing cyber data is the best way to understand the marketplace, allowing the state insurance regulators to understand the commonly used exclusion language or policy limitations.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024\_Fall/WG-Cybersecurity/2024 1030Interim-Meeting/Minutes-CyberWG103024.docx

# 2. Hear Comments on the Confidential Cybersecurity Event Repository & Portal (CERP)

**Attachment B**

*–Cynthia Amann (MO)*

## **Streamlining Cybersecurity Event Reporting for the US Insurance Sector: A Two-Phase Approach**

This document outlines a proposal for the development of a confidential Cybersecurity Event Repository and Portal by the NAIC, aimed at enhancing the cybersecurity event notification process within the US insurance sector. The initiative seeks to improve the reporting process, ensure robust confidentiality, and achieve regulatory convergence by implementing a centralized portal in two phases: initial testing and subsequent full-scale implementation. This approach addressed the current challenges of regulatory fragmentation and aims to provide a secure, efficient, and unified portal for handling cybersecurity event notices.

The regulators are intending that the portal would:

- Initially be focused on facilitating the transmission of event notices pursuant to the Insurance Data Security Model Law #668 (MDL-668).
- Information provided by companies to regulators via the portal would be focused on the MDL-668 reporting requirements.
- Include functionality allowing for the submission of updates to the initial notice to the Department.

Accordingly, the regulators are asking for input from the public as this idea advances before considering formal action. Any comments received will be made available publicly ahead of the National Meeting. If you wish to submit written comments, please send them to our NAIC staff Koty Henry ([khenry@naic.org](mailto:khenry@naic.org)) by November 15<sup>th</sup> or indicate a plan to speak at the National Meeting, so the agenda can be adjusted to allow for public input.

The language from the meeting is provided below. Input may include:

- Suggestions for functionality that would help make a portal successful for regulators and for companies utilizing the portal for event notice submissions.
- Suggestions on existing state portals that may provide a useful model for the NAIC to consider as it studies the development of an NAIC portal.
- Suggestions on the sequence of the initiative, including milestones at which public input would be meaningful.

### **Two Motions for One Project – Actions anticipated provided for context**

#### **1) First**

- **Goal:** NAIC creates a minimally functional portal to test security and access controls.
- **Focus:** States that have adopted MDL-668.

#### **2) Second**

- **Goal:** Implement the portal for states with MDL-668; Plan improvements for regulatory convergence.

## Background

- **CERP:** Provides guidance on the cybersecurity event notification process.
- **One-to-many Report problem:** Current regulatory fragmentation adds risk and complicates MDL-668 adoption.

## Current Status:

- **Technical Feasibility:** NAIC has the necessary technical feasibility and practical experience of maintaining confidentiality through robust security and access controls.

## 1) Motion to Build, Test & Survey

- **Build Plan:** Develop a minimal portal meeting MDL-668 requirements and test its confidentiality capabilities.
  - o Limited to states with MDL-668 and specific questions in Section 6B.
  - o Challenges in some states with unique requirements not covered by MDL-668.
- **Testing Plan:** Use AI- generated data and tabletop exercises to simulate performance and cybersecurity events and demonstrate confidentiality capabilities of the portal.
- **Survey & Converge:** Concurrently to testing, collect Information to understand state specific implementations of MDL-668 and align portal design with existing legislation.

## 2) Motion to Implement & Improve

- Implement a minimal portal to reduce regulatory burden by providing a robustly tested centralized repository.
- Plan for future enhancements to achieve regulatory convergence and allow for updates to be made for functionality.



November 15, 2024

Cynthia Amann, Chair  
Michael Peterson, Vice Chair  
Cybersecurity (H) Working Group  
National Association of Insurance Commissioners  
1100 Walnut Street  
Kansas City, MO 64106-2197

*Attn: Koty Henry, Cybersecurity Policy Advisor, P&C Regulatory Services; Miguel Romero, Director, P&C Regulatory Services*  
Via email: [khenry@naic.org](mailto:khenry@naic.org)

*RE: ACLI Comments to Cybersecurity (H) Working Group Event Repository Two-Phase Approach*

Dear Chair Amann and Vice Chair Peterson:

The American Council of Life Insurers (ACLI) appreciates the opportunity to respond to the Cybersecurity (H) Working Group's continued efforts to create a Cybersecurity Event Repository Portal. ACLI supports the NAIC's continued work to combat the threat of cybersecurity events and the impact these events have on insurance companies and consumers by targeting a key issue, the "one-to-many" notification issue. We appreciate the Working Group's engagement in circulating this two-phase approach and hope to continue offering stakeholder input during this important process. There are three key member concerns: 1) confidentiality of information provided and shared, 2) security of the portal, and 3) continued stakeholder input and transparency during this process.

### **Confidentiality of Information Provided and Shared**

The Working Group's commitment to keeping confidentiality at the forefront of these discussions is encouraging and necessary. While this tool will be useful to all parties involved and will provide a strong consumer benefit in secure handling of cybersecurity incident response, it also presents an opportunity for confidential information to be shared with those who are not intended as the recipient. We reiterate that the testing phase should be thorough and should specifically address who would have access to the information shared. In particular, keeping the recipients only to those states impacted by the event and who have also adopted Model 668 is key. We are pleased with the outlined limited approach as an initial measure to combat confidentiality concerns.

---

American Council of Life Insurers | 101 Constitution Ave, NW, Suite 700 | Washington, DC 20001-2133

---

The American Council of Life Insurers (ACLI) is the leading trade association driving public policy and advocacy on behalf of the life insurance industry. 90 million American families rely on the life insurance industry for financial protection and retirement security. ACLI's member companies are dedicated to protecting consumers' financial wellbeing through life insurance, annuities, retirement plans, long-term care insurance, disability income insurance, reinsurance, and dental, vision and other supplemental benefits. ACLI's 280 member companies represent 94 percent of industry assets in the United States.

## **Security of the Portal**

We understand the NAIC is very experienced in handling sensitive information and we appreciate the seriousness with which this Working Group is testing this process. Keeping this as a key priority will benefit all parties involved as this portal will contain sensitive information that could be viewed as a vulnerable target.

## **Continued Stakeholder Input**

We appreciate this opportunity to provide input at this initial stage. The two-phase approach is promising and we would ask that we are able to receive updates and provide input during the very important Phase I process. We are also looking forward to hearing more about this approach at the Fall National Meeting. Transparency during this process will aid in further understanding and will provide ACLI members with the opportunity to give helpful insights on the event notification process.

Thank you again for the thoughtful creation of this much-needed portal. We look forward to further discussions, input, and updates. Please do not hesitate to reach out if there is a specific area of member input that would be beneficial.

Thank you,

Kirsten Wolford  
Counsel, Cybersecurity and Privacy  
ACLI  
[kirstenwolford@acli.com](mailto:kirstenwolford@acli.com)  
(202) 624-2059

**From:** [Motter, Miranda](#)  
**To:** [Henry, Koty](#)  
**Cc:** [Motter, Miranda](#)  
**Subject:** FW: [External Email] Proposal for Confidential Cybersecurity Event Repository & Portal  
**Date:** Friday, November 15, 2024 1:28:49 PM  
**Attachments:** [image001.png](#)  
[image002.png](#)  
[image003.png](#)  
[image004.png](#)  
[image005.png](#)  
[103124 Messaging to Cybersecurity Working Group.pdf](#)

---

**CAUTION:** This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

November 15, 2024

Ms. Cynthia Amann  
Chair, Cybersecurity (H) Working Group  
National Association of Insurance Commissioners  
1100 Walnut Street, Suite 1500  
Kansas City, MO 64106

Via email to [Koty Henry](#)

**Re: Proposed Confidential Cybersecurity Event Repository and Portal**

Dear Ms. Amann;

AHIP appreciates the opportunity to offer comments following the recent Cybersecurity (H) Working Group's presentation by Koty Henry on a proposal for the creation of a Confidential Cybersecurity Event Repository and Portal (the "Portal") to provide a uniform means of reporting cybersecurity events in those states which have enacted the NAIC's Insurance Data Security Model Law, #668. We offer these suggestions and questions:

- Regulators should develop the Portal to include deference to existing federal information security reporting requirements for health plans and reduce duplicative reporting requirements by synchronizing with existing obligations to agencies such as the Federal Trade Commission (FTC), U.S. Health and Human Services (HHS), Cybersecurity and Infrastructure Security Agency (CISA), and the Securities and Exchange Commission (SEC).
- How would the Portal operate in situations involving reportable cybersecurity events in multiple states? Would all states be required to accept the Portal-prescribed information? How would the Portal be adaptable to accommodate reports which described differing impacts from state to state?
- If a reporting portal is pursued, it is important for NAIC to ensure an adequate level of confidentiality and security protection to comply with #668's provisions and to limit data collection to the minimum necessary in alignment with HIPAA regulations.

We thank you again for this opportunity.

Sincerely,

Miranda Motter  
AHIP  
Senior Vice President, State Affairs and Policy

Miranda Creviston Motter, JD  
Senior Vice President, State Affairs and Policy  
c 202.923.7346  
[mmotter@ahip.org](mailto:mmotter@ahip.org)

AHIP – Guiding Greater Health  
601 Pennsylvania Avenue, NW, South Building, Suite 500  
Washington, D.C. 20004  
[ahip.org](http://ahip.org) | [Twitter](#) | [Facebook](#) | [LinkedIn](#) | [Instagram](#)

---

**From:** Henry, Koty <khenry@naic.org>  
**Sent:** Thursday, October 31, 2024 6:31 PM  
**Cc:** Henry, Koty <khenry@naic.org>; Romero, Miguel <MARomero@naic.org>  
**Subject:** [External Email] Proposal for Confidential Cybersecurity Event Repository & Portal

**To the Members, Interested Regulators, and Interested Parties of the Cybersecurity (H) Working Group**

As a follow up to our Cybersecurity (H) Working Group meeting yesterday, attached is the proposal for the development of a confidential Cybersecurity Repository and Portal aimed at enhancing the Cybersecurity event notification process within the insurance sector. This initiative is designed to meet the needs of both industry and regulators by splitting the project into two steps as described in the attached document which will be posted on the working group's page by early next week.

Your feedback on the sequence and details of this proposal are valued, please share your thoughts and suggestions to ensure we address all stakeholder requirements effectively. Written comments can be sent to me by November 15<sup>th</sup>. If you plan to speak at the National Meeting, please indicate so we can adjust the agenda accordingly.

Respectfully,  
Koty

November 15, 2024

NAIC Cybersecurity (H) Working Group  
NAIC Central Office  
1100 Walnut Street  
Suite 1500  
Kansas City, MO 64106  
Via email: khenry@naic.org

RE: Proposal for Confidential Cybersecurity Event Repository & Portal

Dear Chair Amann, Vice Chair Peterson, and Members of the Cybersecurity Working Group:

Thank you for this opportunity to provide feedback regarding the NAIC Cybersecurity Working Group proposal for the development of a confidential Cybersecurity Repository and Portal.

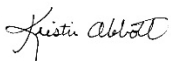
APCIA<sup>1</sup> generally supports the idea of a uniform method of notifying state regulators of data breaches. When insurers experience a cybersecurity event that spans multiple states, they are faced not only with containment and response, but also with navigating the various state reporting portals and differing requests for information. A centralized reporting portal would potentially streamline this process. However, it is important that such a portal be secure, that all data be kept confidential, and that any submitted notices be shared only with the intended regulatory bodies.

Recognizing that the threshold question must be whether the NAIC can maintain a secure portal, we agree that before spending considerable time and energy on the project the first step should be to build and test security and access controls as outlined in the first motion. Should the testing successfully show that the NAIC can build and maintain a secure portal, more time should then be taken for all stakeholders to discuss the functionality of the portal, including how the portal will be used and how submissions will be shared. For that reason, we propose suspending consideration of the second motion for a later date. APCIA welcomes the opportunity to serve as a resource to the Working Group as you continue this endeavor.

Please do not hesitate to contact us with questions.

Thank you,

Kristin Abbott



---

<sup>1</sup> The American Property Casualty Insurance Association (APCIA) is the primary national trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA represents the broadest cross-section of home, auto, and business insurers of any national trade association. APCIA membership consists of over 1,200 member companies (or over 300 member groups). APCIA member companies P&C countrywide market share is 65% (total 73% commercial lines, 55% personal lines).

November 15, 2025

Cynthia Amman (MO), Chair  
NAIC Cybersecurity (H) Working Group  
c/o Koty Henry, NAIC Cybersecurity Policy Advisor, P&C Regulatory Services  
Via email [khenry@naic.org](mailto:khenry@naic.org)

Re: NAMIC Comments on the Proposed Cybersecurity Event Repository and Portal

Dear Chair Amman, Vice-Chairs, and Members of the Working Group:

On behalf of the National Association of Mutual Insurance Companies (NAMIC)<sup>1</sup>, we would like to thank the NAIC Cybersecurity Working Group for requesting and accepting comments on the proposed Cybersecurity Event Repository and Portal for the US Insurance Sector.

NAMIC appreciates the Working Group identifying a need for efficiency as it relates to the cybersecurity event notification process detailed in Section 6 of the Insurance Data Security Model Law #668, and the Cybersecurity Event Response Plan (CERP). *The ability to have an easier, more streamlined way to report notifications of cybersecurity events is a well-intentioned goal; yet it is a goal that may also present substantial, systemic risk if not both: 1) intentionally narrow in breadth and function; and 2) structured with strong security and governance protocols.* In this vein, NAMIC provides below general inquiries and substantive comments on the portal proposal.

## SUBSTANTIVE COMMENTS

### Agreement that the Current System is Unsustainable

NAMIC recognizes and agrees with the Working Group that the current reporting system across jurisdictions is burdensome for insurers. In the midst of investigating, handling, and responding to a cybersecurity event, licensees are required to notify both consumers and numerous jurisdictions, some with varying requirements for reporting, taking valuable resources away

---

<sup>1</sup> The National Association of Mutual Insurance Companies consists of nearly 1,500 member companies, including seven of the top 10 property/casualty insurers in the United States. The association supports local and regional mutual insurance companies on main streets across America as well as many of the country's largest national insurers. NAMIC member companies write \$391 billion in annual premiums and represent 68 percent of homeowners, 56 percent of automobile, and 31 percent of the business insurance markets. Through its advocacy programs NAMIC promotes public policy solutions that benefit member companies and the policyholders they serve and fosters greater understanding and recognition of the unique alignment of interests between management and policyholders of mutual companies.



from addressing the cyber event itself. Without a reasonable solution for the future, the regulatory and administrative burden may only continue to grow as more states adopt Model # 668, or their own separate insurance data security requirements.

### Centralized Data Repository Risk

Before considering and voting on the steps of the portal project, NAMIC asks the Working Group to first consider the substantial and systemic risk of centralizing sensitive cybersecurity event information, and whether the need for efficiency in cybersecurity event reporting should overtake the very cybersecurity aspects that stakeholders are looking to protect.

The Working Group's stated intent for the portal is that the portal would facilitate the transmission of event notices including submission of updates to the initial notice. Given this intended functionality, insurers would be entering information into the portal, and that data would presumably be housed in this centralized repository. While this would facilitate a streamlined notification experience, it also introduces a sensitive information target and vulnerability for the industry at large, including the NAIC and Regulators who share a responsibility to protect consumer information.

Even with stringent controls and tabletop exercises as the Working Group is proposing, we are faced with the reality that cyber criminals continue to carry out more sophisticated attacks, and the financial services industry continues to be a prime target, given the sensitive information it holds, and the role it plays in society. ***By centralizing the most sensitive substantive breach response measures and information, the portal may be a prime target for cyber criminals to gain access to valuable information on how they can devise new infiltration techniques and compromise insurance industry systems, and it may create an opportunity to exploit other companies' vulnerabilities.***

Given the risk of centralizing sensitive vulnerability information, the Working Group's portal proposal may inadvertently create a systemic vulnerability, or a target for criminals to obtain information on a broad swath of the financial services industry.

### Recommendation to Bifurcate the Response from the Vulnerability Information

As an alternative to a centralized database or repository with vulnerability information on the issue, NAMIC suggests the Working Group consider a platform for *management* of the issue – through bifurcating the procedural aspects from the substantive, vulnerability information.

By narrowing the scope of the proposal in both breadth and function, some streamlining of the reporting process may be achieved, while also protecting the more vulnerable and sensitive information included in reports through avoiding one comprehensive centralized database.



*By way of one example, the centralized portal could be a location where licensees provide initial notice to departments that an event has occurred, without including the sensitive substantive information called for in Model #668.* For purposes of illustrating this example, a licensee subject to Model # 668 that experienced a reportable event could submit to the portal that an event has occurred. Separately, as the Working Group may consider, the licensee could then work directly with a lead regulator to provide the substantive information called for in Section 6. B. of Model # 668. This example provides some streamlining to the report process, in that a licensee would not need to initially submit all information to a number of different departments, but the substantive report to the lead regulator, and pared down notice information to the portal. With the portal being an avenue for initial notification, relevant departments would then be able to contact the lead regulator and/or follow up with the licensee for the detailed reporting information. We ask the Working Group to consider whether something like this would meet the efficiency need being sought after.

*As an alternative option to total bifurcation of process and substance, the Working Group, in conjunction with stakeholders, might consider selecting only certain substantive items be included for submission to the portal.* Specifically, sub. (10) and (11) of Section 6. B. in Model # 668 are items that the Working Group might consider as more vulnerable information that could be excluded from submission to a centralized repository and portal. Instead, the Working Group might consider having that information be reserved for a licensee's lead regulator, or information that regulators could be referred to the licensee directly to obtain through relevant authorities. In the portal, a licensee might instead indicate, for example: 1) for sub. (10) that the licensee does or does not yet have those results; and 2) for sub. (11) provide a contact for this sensitive information on the description of the efforts. If this alternative option be one the Working Group pursues, we ask the Working Group to engage in a stakeholder comment process for comment on the specific pieces of information that would or would not be included in the repository and portal.

*Through bifurcating the response from the vulnerability information, the sensitive and vulnerable information regarding the breach remains dispersed* – instead of all companies submitting the data to one centralized repository, the data would be submitted to the lead regulator and other impacted state departments subsequently requesting such data (or, conversely, at least the most vulnerable, sensitive information would not be submitted to the portal). To be sure, the example approaches discussed above, much like the portal and repository approach more broadly, only solve for streamlining reporting in those states that have adopted Model # 668. Additionally, some aspects of the examples discussed may not be achievable without potentially reopening Model # 668. But, conversations around potential alternatives that still provide for efficiency, while acknowledging and solving for unintended systemic risk, are ones we encourage the Working Group to have and solve for ahead of embarking on the project.

#### Governance and Information Security Protocols

Taking all of this a logical step further, though the Working Group has stated confidentiality requirements are technically feasible, there are a number of governance and information security aspects that would need to be identified and implemented.





Thus far, we've not seen anything regarding the development of strong protocols, governance, and information security standards happening in parallel with the portal development and discussion. *For instance, who would have permissions to access the information, and what would be the justified need for such access and permission?* Would individuals other than the relevant state departments for an event (for instance, staff or others at the NAIC) also have access to the information? If so, under what circumstances and justifications would those individuals have such access?

*From a confidentiality perspective, we would encourage the Working Group to examine and make clear the authority by the state that allows for confidentiality, whether it is specific to market conduct, IT exams in the financial context, or authority through other laws like Model # 668.* We also ask that the Working Group ensure that any specific information sharing agreements in and amongst the NAIC and states specific to this project be in the overall repository and portal ecosystem prior to making any repository and portal live for use. These are merely a couple of examples that we ask the Working Group to consider, in the vein of providing certainty in the integrity of the system and the protections it affords.

#### IN SUMMARY

We close by again thanking the Cybersecurity Working Group for allowing NAMIC to submit comments to engage on this extremely important discussion, and we urge you to continue offering additional iterative opportunities for robust, transparent conversations with industry throughout the process. NAMIC endeavors through these comments to point out concerns over security of report information and attempt to offer some examples of how the portal could be used to streamline processes, but as an initial report mechanism, rather than centralized repository of sensitive vulnerability information. We ask that, if the Working Group is moving forward with the proposal, that it not advance the launch of the portal until there is consideration of lesser risk alternatives, designating a lead regulator being one example, and having thorough discussions and solutions over security vulnerabilities. NAMIC looks forward to continuing our work with the Working Group to arrive at solutions that protect and benefit all stakeholders.

Sincerely,

Lindsey Klarkowski  
Director of Data Science & AI/ML Policy  
NAMIC

November 15, 2024

Cynthia Amann, Chair  
Cybersecurity (H) Working Group  
National Association of Insurance Commissioners  
c/o Koty Henry  
Cybersecurity Policy Advisor  
Via email [khenry@naic.org](mailto:khenry@naic.org)

RE: RAA Comments on the CERP Two-Phase Approach

Dear Chair Amann,

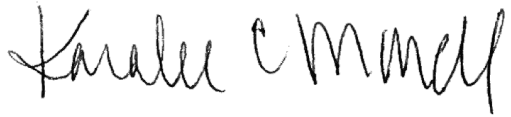
The Reinsurance Association of America (RAA) appreciates the opportunity to submit comments to the Cybersecurity (H) Working Group on the document outlining the two-phase approach to the implementation of a confidential Cybersecurity Event Repository and Portal (CERP). The Reinsurance Association of America (RAA) is a national trade association representing reinsurance companies doing business in the United States. RAA membership is diverse, including reinsurance underwriters and intermediaries licensed in the U.S. and those that conduct business on a cross-border basis. The RAA also has life reinsurance affiliates and insurance-linked securities (ILS) fund managers and market participants that are engaged in the assumption of property/casualty risks. The RAA represents its members before state, federal and international bodies.

The RAA seeks mainly to comment on the sequence of the initiative and when public input would be meaningful. The RAA is concerned about the ability to keep the portal secure and wants there to be the time and ability for meaningful comment at each stage in this process to ensure the portal will be secure. Because of this the RAA supports bifurcating the two-phase approach and answering each question one at a time. Bifurcating the approach will ensure there is both ample time for stakeholder feedback and that the repository can be completely secure.

The first focus should be on solely if the NAIC can maintain a secure portal and repository with ample time for stakeholder feedback. The RAA believes that since such a repository does not necessarily further the purpose of insurance regulation, financial solvency and consumer protection, a repository should only be created if it is completely secure. If the Working Group is ready to advance the RAA believes solely focusing on the security question initially is the best approach. After resolving this first question the Working Group will have the information it needs to discuss the subsequent development and implementation of such a portal. The RAA believes the security of the portal remains paramount as such a portal would create risk and burden for organizations experiencing cyber events.

The RAA looks forward to continuing to work with you on this important project. We would be happy to meet with members of the Cybersecurity (H) Working Group and NAIC staff to discuss our position in more detail. We look forward to further engagement on these issues.

Sincerely,



Karalee C. Morell  
SVP and General Counsel  
Reinsurance Association of America

# 3. Hear a Presentation from Alvarez & Marsal on Incident Response Management and Lifecycle

## Attachment C

–Scott Harrison (Alvarez & Marsal)

–Rocco Grillo (Alvarez & Marsal) (Virtual)



**Global Cyber Risk Services**

# **Surviving the Firestorm of a Cyber Incident**

**NAIC National Meeting Fall - November 2024**

**ALVAREZ & MARSAL**  
LEADERSHIP. ACTION. RESULTS.™



**ROCCO GRILLO**

**Managing Director  
Global Cyber Risk & Incident Response  
Investigations  
Alvarez & Marsal**

**[rgrillo@alvarezandmarsal.com](mailto:rgrillo@alvarezandmarsal.com)**

**+1.917.693.9700**

## **Presenter**

- Global Cybersecurity Risk and Incident Response Services practice leader.
- Expert in cybersecurity advisory and incident response investigations.
- Provides clients with cybersecurity advisory services, incident response investigations and other technical advice, including providing guidance to C-suite and board members
- Trusted partner with multiple government agencies, including the FBI, USSS, CISA / Homeland Security, and the FTC in investigating a variety of cybersecurity and privacy breaches and has assisted clients with responding to some of the largest cyber-attacks over the last 15 years.
- Member CREST'S Americas Council, Shared Assessments, and served as an affiliate board advisor to industry ISACs.

# Agenda

One  
**01**

# Agenda

---

**Introductions**

---

**State of Cyber**

**5 mins.**

---

**Ransomware Key Considerations**

**10 mins.**

---

**Incident Response Plan Best Practices**

**10 mins.**

---

**Q&A**

**5 mins.**

---



# The State of Cyber

TWO  
02

# 2024 Cyber Threat Landscape & Trends

- **Ransomware - Double and Triple Extortion**
- **Business Email Compromise**
- **Mid-Game Hunting**
- **Intermittent Encryption**
- **Top Intrusion Vectors**
  - Phishing Schemes
  - Stolen (or Brute Forced) Credentials
  - Supply-Chain
  - Unpatched Software
  - Zero Days
- **Underreporting**

# Ransomware Key Considerations

Three  
**03**

# Ransomware Key Considerations

- **Impact assessment** – Determine what is not operational, who will notice, and what consequences will likely follow. Identify any potential “downstream” impacts to clients or vendors.
- **Vendor engagement** – Identify the external legal counsel, forensics firm, negotiation and payment, workforce augmentation/restoration, forensic accountant to document expense and income loss, and communications firms to consider engaging.
- **Threat actor intelligence** – Find the ransom note and make preliminary attribution based on file extension and note content to start analysis of: (1) is this a threat actor known to only encrypt or steal/encrypt; and (2) is this a threat actor who may be on a sanctions list.
- **Ransom negotiation strategy** – Directly or through negotiation, make initial contact with the threat actor to obtain initial demand and then begin to develop negotiation strategy. Identify threat actor’s history of payment default, decryptor efficacy, and tor site data posting strategy. Consider payment logistics (e.g., timing of wiring funds to negotiation vendor before wire close/weekend).
- **Restoration planning** – Determine viability of backups and what alternate restoration options exist.
- **Containment** – Identify how access occurred and how ransomware was deployed, are there systems that should be taken offline to prevent further spread and build plan for eliminating current access so you can restore to a secure environment (or build segmented VLAN to restore in until containment occurs).
- **Preservation** – Account for preservation needs before wiping and reimaging devices during restoration.
- **Communications** – Determine stakeholder communication needs and prepare drafts of reactive holding statement for media, associates, franchisees.
- **“Response Plan” execution** – Align response to key response considerations based on incident, business continuity, and crisis response plans.
- **Notice analysis** – Develop preliminary assessment of potential notification obligations.
- **Documentation** – Identify what insurance carrier(s) (e.g., cyber, kidnap/ransom) will require to give consent to ransom payment and to reimburse (e.g., “business case” for payment, OFAC clearance report).

# Incident Best Practices

Four  
**04**

# Incident Response Plan Characteristics & Best Practices

- ✓ Involving key stakeholders, clear definition of roles and responsibilities, and decision-making protocols;
- ✓ Clear escalation paths;
- ✓ Informed decision making;
- ✓ Well defined understanding of business impact;
- ✓ Processes for both internal / external communications;
- ✓ Understanding third party / external relationships;
- ✓ Technology support for investigative purposes / analysis;
- ✓ Ongoing enhancements to an IR policy in response to embracing new technologies, increasing sophistication in attacks, and the evolving regulatory landscape





# 4. Hear Updates on its Workstreams

- A. Data Calls and Definitions—*Colton Schultz (ND)*
- B. *IT Examination (E) Working Group/Exhibit C Drafting Group Progress—Shane Mead (KS)*
- C. *Coordination with the Academy and Other Related Efforts—Wanchin Chou (CT)*
- D. *CERP/Insurance Data Security Model (IDSM) Survey—Michael Peterson (VA)*



# 5. Hear a Summary of its 2024 Activities and a Preview of its 2025 Work Plan

**Attachment D**

*–Cynthia Amann (MO)*

# Cybersecurity Working Group '24

- At the Spring National Meeting, the Working Group adopted the Cybersecurity Event Response Plan, to aid state insurance supervisors respond to cybersecurity events impacting the insurance industry.
- At the Summer National Meeting we heard a panel with guests from Coalition, Aon, and Arch Reinsurance, discussing cyber insurance marketplace trends and cyber insurance has grown to be more than just a mechanism to transfer financial risk, its become a market-based tool to drive security improvements across businesses and infrastructure.
- We have met with and heard from multiple federal agencies, other regulators, and industry experts discussing market trends, the evolving cyber-risk & threat landscape, and the effectiveness of security controls.
- Today we heard from Alvarez & Marsal, the knowledge and experience they were able to share helps building the solid foundation of education and awareness efforts we pursued this year.

# Cybersecurity Working Group '25

- Continuing into 2025, our efforts to create a centralized reporting portal at the NAIC will focus initially on the language within MDL-668.
  - Once the limited repository's security and confidentiality concerns are addressed, other enhancements and improvements can be made to align with regulatory convergence.
- We will continue to invite presentations from industry professionals and appropriate subject matter experts, as we look to better understand cyber insurance coverage and underwriting enhancements as well as cybersecurity landscape trends.
- Two charges have been added for 2025.
  - Coordinate with NAIC to facilitate intelligence driven cybersecurity tabletop exercises with state departments of insurance providing input on scope and timing, as necessary.
  - Consider updates and developments, provide technical assistance, and advise NAIC staff in the production of the Cyber Insurance Report.