NATIONAL MEETING
SPRING / PHOENIX
2024
NAIC

CYBERSECURITY (H) WORKING GROUP

Sunday, March 17, 2024

2:30 – 3:30 p.m.

Phoenix, AZ

Consider Adoption of the Nov. 16, 2023 Meeting Minutes

Draft: 11/20/23

Cybersecurity (H) Working Group
Virtual Meeting
November 16, 2023

The Cybersecurity (H) Working Group met Nov. 16, 2023. The following Working Group members participated: Cindy Amann , Co-Chair and Kim Dobbs, Jo LeDuc, and Brad Gerling (MO); Gille Ann Rabbin, Co-Chair and Hesham El-Meligy and Joanne Berman (NY); C.J. Metcalf, Co-Vice Chair, (ND), Michael Peterson, Co-Vice Chair (VA); Julie Jette (AK); Chris Erwin (AR); George Bradner, Wanchin Chou, Anthony Francini, Qing He, Jennifer Miner, Kurt Swan, and Kenneth Roulier (CT); Tim Li (DE); Paula Shamburger and Tia Taylor (GA); Lance Hirano (HI); Daniel Mathis and Logan Thomsen (IA); Shane Mead (KS); Jackie Horigan (MA); Kathryn Callahan and Mary Kwei (MD); Jeff Hayen, Isaac Kane, Joe Keith, Jason Tippett, and Danielle Torres (MI); Troy Smith (MT); Tracy Biehn (NC); Colton Schulz (ND); Martin Swanson (NE); Don Layson and Matt Walsh (OH); Mary Block and Karla Nuissi (VT); Tarik Subbagh (WA); Also participating were: Yada Horace (AL); Philip Gates (CO); Anoush Brangaccio, Kun Chen, and Ronald Waye (FL); Victoria Hastings (IN); Jackie Horigan (MA); Daniel Lawson and Vaness Sullivan (ME); David Bettencourt (NH); Mike , Sebastian Conforto, and Jodi Franz(PA); Joseph Rapczak, Matt Gendron, and Patrick Smock (RI); Allan McVey (WV); and Lela Ladd (WY).

1. Adopted its Summer National Meeting Minutes

Schultz made a motion, seconded by Mead, to adopt the Working Group's March 7 minutes. (*see NAIC Proceedings – Spring 2023, Innovation, Cybersecurity, and Technology (H) Committee, Attachment Two*). The motion passed unanimously.

2. Discussed the Comments Received and Heard an Update on the Cybersecurity Event Response Plan (CERP) Drafting Group

Amann said the comments received have been taken into consideration and drafted into the draft document being reviewed today.

The Working Group welcomes comments, either written comments or verbal comments during this call. Amann asked Miguel Romero (NAIC), to walk through the draft and provide high-level comments on what has changed. Text was added to the end of the Introduction section of the document to remind state insurance regulators of other reporting requirements in a state, for example, the state's Attorney General (AG) or other overlapping laws. A sentence was added at the end of the section to support and encourage using the Lead State concept, where possible and appropriate.

Based on the comments received, a sentence was added to the end of the first paragraph in the "Forming a Team and Communicating with Consumers" section to address the need for communication to be coordinated and consistent with the messaging provided by the affected licensee prior to any consumer communication so that the consumer will receive the correct information.

An "Overview of Lead State Concept" section was added to the CERP document. This section introduces the lead state concept, as well as some reference resources included in the text from the *NAIC's Financial Condition Examiners Handbook* and the *NAIC's Market Regulation Handbook*. This section does not provide the state using the CERP a mandate, but it might be beneficial to DOIs.

At the end of the “Understanding and Receiving Notifications” section, language was added to make it clear that licensees have the responsibility of updating and supplementing previous notifications about material changes to previously provided information to the extent possible. A sentence addressing events that originated with a vendor.

A new section, "Data Minimization,” was added to the CERP. This section explains data minimization and adds confidentiality language in response to comments from interested parties. The comments reflected that confidentiality is not just about trade secrets but includes other confidential information that must be protected. The section also addresses that DOIs should limit the collection of information to that which is adequate and directly relevant, as well as necessary to accomplish a specific purpose.

Amann stressed that this document is meant to provide sufficient information to state insurance regulators, whether they are well-versed regarding cybersecurity or those who are new to cybersecurity oversight. While there are still details to be addressed in the current draft of the CERP, the Working Group has incorporated industry comments received to date. The plan is to have a couple of states pilot using the CERP and provide feedback. In 2024 the Working Group will hear from experts and other bodies to discuss their role in responding to security events. NAIC staff are to talk to some of the NAIC Working Groups for their input regarding how the lead state concept might best be added to this document.

Cate Paolino (National Association of Mutual Insurance Companies—NAMIC) stressed that the lead state concept is important because it helps to increase consistency. Romero asked Paolino and other interested parties to provide input regarding the lead state concept and to provide any thoughts as to whether there is any inconsistency in the use of the lead state concept.

Kristen Wolfford (American Council of Life Insurers—ACLI) said ACLI encourages additional language stating that the DOIs should speak through the licensee's head contact. Additionally, ACLI believes there should be consideration of adding language that indicates that the most accurate information is provided by establishing a clear avenue and making sure that the DOIs are not providing forms directly to outside counsel or third-party mitigation firms. Information could still be conveyed to the outside counsel but should occur through the licensee to be sure privilege is being preserved while everyone is abreast of what is transpiring.

Shelby Schoensee (American Property Casualty Insurance Association—APCIA) said that APCIA is supportive of the lead state concept.

Bob Ridgeway (America’s Health Insurance Plans—AHIP) said it is important for state insurance regulators to consider that there are other state law requirements where licensees may need to do further reporting. Most, if not all, states have an attorney general’s law that calls for a breach to be reported to the attorney general. Some licensees may also have to respond to the Gramm Leach Bliley Act (GLBA) requirements. Health insurers have at least three layers of reporting which include 1) HIPAA; 2) the Critical Infrastructure Act of 2022; and 3) the Federal Trade Commission's (FTC) recent health breach notification rule.

Ridgeway said some of AHIP’s members are concerned they would be penalized if they did not get all the reporting to the DOI in full. He reminded his members that the *NAIC Insurance Data Security Model Law* (#668), as well as the amended versions in various states, partial reports are expected because state insurance regulators acknowledge that a licensee will not have all the information when providing the initial notification.

AHIP is also concerned that the confidentiality provided in Model #668 may not give full protection to information that a state insurance regulator shares with a third-party consultant. AHIP has requested some additional language to be added to the CERP to emphasize state insurance regulators are conscious that providing information to third-party consultants will not increase confidentiality risks.

Peterson said there are efforts at the NAIC level, as well as the U.S. and international level, among financial regulators to solve the problem of the one-to-many relationship between states and insurers when it comes to investigating breaches. The most prominent effort existing among the Financial Stability Board (FSB) is the Format for Incident Reporting Exchange (FIRE) concept.
Peterson said the lead state concepts come from group examinations, which come from threats to enterprise risk insolvency. He said the Working Group is going to work on solving these problems in the CERP's guidance.

Amann said the Working Group welcomes further comments. She said the important thing for state insurance regulators to remember is that the first step for a licensee following a breach is to identify and mitigate the issue.

NAIC staff is to clarify and provide more language around communication between private law firms and state insurance regulators.

3. Heard a Presentation on the NIST Cybersecurity Framework

John Boyens (National Institute of Science and Technology—NIST) said NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

NIST has over 3,400 federal employees and about 3,500 guest researchers from around the world.

Both the congressional and executive branches of the government depend on NIST for their technical excellence. The National Security Agency (NSA) uses NIST standards and guidelines as their foundation and then adds more rigorous controls beyond NIST.

Around 2013, there was an executive order that charged NIST with developing a framework for cybersecurity for critical infrastructure. NIST hosted five or six workshops around the country and sent two requests for information (RFI). They collected a lot of information and worked with the private sector industry and academia to build the cybersecurity framework.

NIST's biggest challenge when building the cybersecurity framework was to build it at a level that was not so high-level that it was useless while not being so prescriptive that it would not work across all of the critical infrastructure sectors.

NIST started working on the second phase of the cybersecurity framework, CSF 2.0, in February 2022 and has held three workshops to date. NIST has also had multiple concept papers or drafts of some of the content. The latest version of CSF 2.0 was exposed for a comment period ending Nov. 4. NIST is still getting comments submitted to them. NIST is organizing those comments and has not started the adjudication process but hopes to do so soon.

The financial sector created its own profile, which contains a "Govern" function. A category inside the "Govern" function addresses the internal mechanisms of the supply chain. CSF 2.0 is technology neutral. Many categories were taken out of the "Identify" function and put into the "Govern" function.

Boyens said there are no implementation examples or informative references in the framework core. These two aspects are being moved online, as NIST wants the community to be able to add to the informative references.

Many of the "Govern" sub-categories are things that organizations must do internally before they start pushing their supply chain risk management requirements down their supply chain.

Boyens said NIST is hoping to release the final draft sometime in 2024. Amann encouraged the Working Group members to read the submitted comments. She said these comments provide an idea of how quickly cybersecurity is infiltrating all aspects of business.

A question in the chat asked if NIST works with the Federal Risk and Authorization Management Program (FedRAMP), and if so, what is the involvement. Boyens said NIST helped stand up FedRAMP from their standards. NIST set up the first instance of what the requirements would be for FedRAMP and got their accreditation program set up. Currently, NIST is working on the controls that go into FedRAMP since they are processing, storing, and using federal government data. FedRAMP is required to meet standards and guidelines that NIST produces, so those controls that go into FedRAMP come from NIST.

4. Heard an Update on Federal Activities Related to Cybersecurity

Shana Oppenheim (NAIC) said Senator John Hickenlooper (D-CO) and Senator Shelley Moore Capito (R-WV) have introduced the Insure Cybersecurity Act of 2023. This bill is aimed at helping to better insure small businesses against cyberattacks. The Act would direct the National Telecommunications and Information Administration (NTIA) to create a dedicated working group to develop recommendations for insurers, agents, brokers, and customers to improve communications regarding cybersecurity insurance coverage. It would also direct the publications of easily understandable resources on cybersecurity insurance. The bill was supposed to be marked up this week but was indefinitely postponed.

The executive office of the president's office of the National Cyber Director issued a request for information on cyber regulation harmonization in July. The Office of National Cyber Director (ONCD) is seeking input from stakeholders to understand any existing challenges with regulatory overlap and inconsistencies to explore a framework for reciprocal recognition by regulators of compliance with common baseline cybersecurity requirements. This effort may be intended to harmonize state and federal requirements on examination guidance.

The U.S. Securities and Exchange Commission (SEC) proposed a cybersecurity regulation in July. A final rule was adopted, requiring publicly listed companies to comply with numerous incident reporting requirements and government disclosure requirements. The rules require registrants to disclose material cybersecurity incidents that they experience and to disclose material information about their cybersecurity, risk management, and governance annually. The commission has also adopted rules requiring foreign private issuers to make comparable disclosures.

The Government Accountability Office (GAO) released a cybersecurity program audit guide in September. This guide provides auditors with methodologies, techniques, and audit procedures needed to evaluate the components of an agency's cybersecurity program and system. The guide also includes risk management and incident response.

The GAO issued a critical infrastructure protection national security strategy in September addressing the protection of critical infrastructures, such as water and electricity, from cyberattacks as a national priority. They recommended monitoring federal cyber initiatives and assessing the agency's current information-sharing methodologies to help address cybersecurity challenges.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2023 Fall/WG-Cybersecurity/2023 1116Interim Meeting/Minutes-CybersecurityWG111623.docx

Consider Adoption of the Cybersecurity Event Response Plan (CERP)

Introduction

The Cybersecurity Event Response Plan (CERP) is intended to support a Department of Insurance (DOI) in its response following notification or otherwise becoming aware of a cybersecurity event at a regulated insurance entity (licensee). Early communication with licensees about how a DOI intends to develop their processes, including where and how to send cybersecurity event notifications, will assist with compliance.

This guidance follows the definitions and provisions of the NAIC Insurance Data Security Model Law (MDL-668), specifically the process detailed in Section 6, "Notification of a Cybersecurity Event," and related sections. If a state has made any changes in passing its version of MDL-668 or passed other regulations or legislation, it will need to adjust the guidance herein accordingly. Confidentiality parameters for reported cybersecurity event information vary depending on whether a state has adopted MDL-668, passed its own version of MDL-668, or passed its own legislation. Every state must defer to its specific confidentiality requirements.

Scope

The CERP does not specifically address which events must be reported, as laws and regulations vary from state to state. DOIs should defer to the reporting requirements specific to their state, regardless of whether the state has adopted MDL-668, a revised version, or its own legislation.

Forming a Team and Communicating with Consumers and Licensee Officials

DOIs must establish clear roles, responsibilities, and levels of decision-making authority to ensure a cohesive team response to cybersecurity events at regulated entities. Furthermore, many DOIs have divisions, such as consumer services sections, to inform and protect insurance consumers. In the case of a disruptive cybersecurity event, providing the consumer services section with accurate, up-to-date information and scripts will enable better consumer assistance and will help avoid duplicative or inconsistent information being provided to the public, consumers or otherwise.

Similar to the company's practice of naming a single point of contact to drive communication with a DOI (see "Understanding and Receiving Notifications and Required Information - #13), a DOI may also wish to name a single point of contact who can help coordinate inquiries on behalf of the DOI to the licensee.

Communication with Law Enforcement and Other Regulators

During a cybersecurity event, law enforcement agencies and other regulators may request information from the responding DOI. Engaging with law enforcement officials and regulators can benefit overall cybersecurity and inform the DOI's response, provided such communication is permitted under the relevant state regulation.

Understanding and Receiving Notifications and Required Information

States should be mindful that only partial information may be available in the early stages of the information-gathering process. As a licensee's investigation into a cybersecurity event proceeds, new

information may become available, and information previously provided may change.

Section 6 of MDL-668 requires licensees to notify the state insurance commissioner about reportable cybersecurity events and to provide the DOI with as many of the following 13 pieces of information, set out in Section 6(B), as possible, given the relevant state-specific required reporting timeframe:

1) The date of the cybersecurity event.
2) A description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any.
3) How the cybersecurity event was discovered.
4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done.
5) The identity of the source of the cybersecurity event.
6) Whether the licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when such notification was provided.
7) A description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information, or types of information allowing identification of the consumer.
8) The period during which the information system was compromised by the cybersecurity event.
9) The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner [pursuant to this section of MDL-668].
10) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed.
11) A description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur.
12) A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event.
13) Name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

A state may make changes when passing its version of MDL-668 or other legislation that varies from the requirements set out in Section 6(B) of MDL-668. In this case, the state must adjust this guidance to comply with the information it requires a licensee to report under its legislation.

Receiving the information listed above may take some time, and some information may be available earlier than others. Since some information may never be ascertained, like the identity of the source of a cybersecurity event (or other responsible parties), event notifications should be sent out promptly without waiting for all relevant information to be gathered. After a licensee notifies the DOI of the initial cybersecurity event, the licensee can update its notification.

Appendix A of this document, *Cybersecurity Event Notification Form,* provides an optional form that can be used to help states collect information.

The licensee notifying the DOI of a breach is responsible for reporting updated data, as required, in accordance with relevant state law. If the licensee in question is the DOI's domestic licensee, it is the DOI's responsibility to ensure the licensee provides as much of this information as possible.

The license is not required to provide specific documents, such as an investigatory report or other documentation, to comply with the information reporting requirements of Section 6(B). While an investigatory or other document may contain the information required by Section 6(B), Section 6(B) does not require that the documentation itself be provided to the DOI. MDL-668 requires that the licensee need only send a description of the required information.

If a DOI determines that it needs to review the underlying documentation, the DOI may want to consider bringing an investigation pursuant to MDL-668 Section 7(A) in the event this section is applicable. Information received pursuant to an investigation brought under Section 7(A) is subject to greater confidentiality protection. If Section 7(A) or a similar section is not applicable, the DOI may consider opening a limited-scope investigation or another similar style of examination that provides explicit confidentiality protection to a licensee. To the extent a DOI wishes to gather information beyond the required information listed above, either through an examination or otherwise, DOIs may wish to minimize information requests to the minimum necessary information needed to perform the examination.

Notwithstanding anything provided in this CERP, a DOI must comply with its responsibilities under MDL-668 Section 8, "Confidentiality," or with the confidentiality requirements in its own legislation, and ensure that all reported cybersecurity event data is properly secured.

Process for Responding to Cybersecurity Events

A DOI's process of responding to a licensee's cybersecurity event should allow it to consistently gather as much required information as possible without unduly burdening the licensee, and a DOI's engagement with a licensee may vary depending on the facts and circumstances of each cybersecurity event. To illustrate, consider three general points where a DOI can engage with a licensee after a cybersecurity event: 1) upon receiving notification or becoming aware of the event; 2) after the DOI's initial investigation; or 3) upon the DOI's completion of the investigation. Some questions a DOI should consider when making the determination of when to engage with the licensee include:

- What is known about the compromise, and is there an ongoing threat?
- Is there a greater threat to the insurance industry (e.g. through the involvement of third-party software many insurers use)?
- Has the licensee lost the ability to process transactions? Can they process claims? Premiums?
- Can the licensee communicate with policyholders? Are their telephones, email, and website working?

- Has the licensee engaged in any general communication with policyholders? Is the licensee able to post a notice on its website? If so, when was the notice posted?
- Has law enforcement responded to the licensee's situation? Are they on-site?
- Are there other professionals on-site assisting with the recovery? What are their roles?

For a cybersecurity event that has been remediated and had a limited impact on daily operations and information technology (IT) operations, the DOI may consider allowing the licensee's investigation to run its course before engaging to obtain any necessary information.

Cybersecurity events that have occurred at a third-party service provider require a different approach by the DOI. Often, a licensee will avail itself of MDL Section 6(D)(3), which allows a third-party service provider to fulfill its notification or investigative requirements pursuant to the terms of an agreement with a licensee. In any event, the licensee must acquire the information required to be reported from the third-party service provider.

If a DOI determines that further investigation is appropriate to ensure policyholder data has been secured, an examination by the DOI of the licensee's response and remediation of the cybersecurity event may be warranted. There are several investigative options available to a DOI, summarized in a document titled "*Summary of Cybersecurity Tools,*" which is maintained by the NAIC's Cybersecurity (H) Working Group under the "Documents" tab on the Working Group's page. These tools include:

- Using the Powers of the Commissioner to examine and investigate and take appropriate enforcement action Under Section 7(A) and (B) described in MDL-668, if adopted and in effect;
- Bringing an investigation via the exam process described in the *NAIC's Financial Condition Examiners Handbook*; and
- Using the following checklists included in the NAIC's *Market Regulation Handbook to assist the DOI's inquiry:*
  - "Insurance Data Security Pre-Breach Checklist," and
  - "Insurance Data Security Post-Breach Checklist"."

A DOI must be prepared to address concerns about the confidentiality and protection of cybersecurity event information that has been reported to it, either under MDL-668 Section 8 or under state confidentiality and information privacy legislation. When a licensee asserts that information required by MDL-668 is exempt from reporting because it falls under the attorney-client privilege, or that information required by MDL-668 constitutes a trade secret, a DOI must consult its legal counsel as to how to proceed.

If a licensee expresses concern about the sensitive nature of a particular document (for example, a forensics report), a DOI should consider performing a formal investigation pursuant to Section 7(A) of MDL-668. As discussed above, documents received pursuant to Section 7(A) of MDL-668 are subject to greater confidentiality protection than is provided by Section 6(B) of MDL-668. If a state's version of MDL-668 does not provide confidentiality protections comparable to those provided by Section 7(A) of the MDL-668, a limited-scope examination to determine compliance with MDL-668 may offer a licensee

similar confidentiality protection.

How to Receive Notifications and Acquire Required Information

There are many options a DOI has for receiving notifications from licensees. DOIs should take reasonable steps to ensure they have proper communication protocols and tools in place in advance of becoming notified or aware of a cybersecurity event. Communication channels established for event notification should provide security for cybersecurity event data-in-transit and data-at-rest, commensurate with the sensitivity of the reported information.

Additionally, DOIs may provide the licensee's outside counsel or third-party mitigation firm, if appropriate, with a form requesting information. As noted above, information may be available at different times throughout the cyber event lifecycle, and notifications can be updated after a licensee makes the initial report.

Appendix A: Sample Template (This is available in Excel):

	Information Requested	**Company Response**
	Company Name	
1	Date of the cybersecurity event.	
2	Description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of third-party service providers, if any.	
3	How the cybersecurity event was discovered.	
4	Whether any lost, stolen, or breached information has been recovered and if so, how this was done.	
5	The identity of the source of the cybersecurity event.	
6	Whether licensee has filed a police report or has notified any regulatory, government, or law enforcement agencies and, if so, when such notification was provided.	
7	Description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information, or types of information	
8	The period during which the information system was compromised by the cybersecurity event.	
9	The number of total consumers in this state affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the commissioner and update this estimate with each subsequent report to the commissioner [pursuant to this section of MDL-668].	
10	The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed.	
11	Description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur.	
12	A copy of the licensee’s privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event.	
13	Name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.	

CERP Comments

ACLI
Financial Security for Life

March 5, 2024

NAIC Cybersecurity (H) Working Group
NAIC Central Office
1100 Walnut Street
Suite 1500
Kansas City, MO 64106

Attn: Cynthia Amann, Chair and Michael Peterson, Vice-Chair, NAIC Cybersecurity (H) Working Group
Via email to Miguel Romero (maromero@naic.org) and Sara Robben (srobben@naic.org)

Re: Cybersecurity (H) Working Group Exposure Draft of the NAIC's Cybersecurity Event Response Plan (CERP)

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 Exposure Draft of the NAIC's Cybersecurity Event Response Plan (CERP). 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. We appreciate the Working Group's engagement in providing further guidance to Departments of Insurance (DOIs) on how to handle cybersecurity event notifications.

There are strong improvements in the most recent draft, in particular the addition of provisions encouraging DOIs to secure data at rest in addition to in transit. Additionally, the emphasis on compliance with confidentiality provisions in Section 8 of Model 668 to keep received information properly secured is an important addition in order to safeguard information in the notification process. Lastly, the inclusion of third party vendor considerations in the "Process for Responding to Cybersecurity Events" section recognizes a key participant in the cybersecurity event process for many companies. We appreciate the Working Group's careful consideration of these issues.

Suggested Revisions to the Cybersecurity Event Response Plan

As you consider adoption of this CERP, we respectfully ask that the Working Group consider further improvements that would lead to a more robust and useful document for regulators and insurance companies alike. The following inclusions would continue to lend to the most accurate information following a cybersecurity event and would more greatly safeguard consumer information.

1. The "Understanding and Receiving Notifications and Required Information" section could be enhanced by adding a provision to encourage DOIs to limit information requests to the minimum necessary to perform its essential functions. In many cases, governmental bodies, such as DOIs, have statutory exemptions

from data privacy and security legislation—creating a less regulated environment with fewer controls to keep data safe. Unnecessarily transmitting or storing consumer data beyond an insurer's control creates undue risk to consumers. ACLI suggests the following language:

- DOIs should carefully consider each request for information and limit those requests to the minimum necessary to perform its essential functions in order to cause minimum risk to consumers.

2. Inclusion of a sentence in the "Forming a Team and Communicating with Consumers" section addressing inconsistent and duplicative notifications would minimize confusion and often inaccurate information spread after a cybersecurity event. ACLI suggests inclusion of the following language:

   - DOIs should take measures to avoid duplicative or inconsistent notifications to consumers in the aftermath of a cybersecurity event.

3. While the emphasis on clear roles within DOIs improves the often-confusing landscape for cybersecurity event notifications, the "Forming a Team and Communicating with Consumers" section would be improved by also including a provision addressing who those individuals should interact with from the licensee side. Additionally, licensees would be better able to notify the correct individuals promptly and accurately if DOIs clearly communicated how and where notifications should be submitted by licensees on their state webpages. ACLI suggests inclusion of the following language:

   - DOIs should make every effort to communicate with the licensee's lead named contact for all communications related to the cybersecurity event to minimize confusion between regulators and licensee. DOIs should include how and where notifications should be submitted by licensees on their state webpages.

4. There are multiple individuals who might have information during and after a cybersecurity event which will be helpful to DOIs. Licensees often rely on outside counsel to provide legal advice which is privileged and confidential and while it is important for DOIs to have all of the information necessary to assess the aftermath of a cybersecurity event, these requests would be best made through the licensee's lead named contact who would be responsible for obtaining the information from outside counsel. ACLI suggests the following revision to the "How to Receive Notifications and Acquire Required Information" section:

   - Additionally, where applicable, DOIs may provide the licensee's lead named contact with a form requesting information from the licensee's outside counsel or third-party mitigation firm.

Lastly, as reflected in the transmittal accompanying the latest CERP draft, addressing the "one-to-many" notification issue could greatly benefit the industry, if effectively implemented. This could cut down on the number of channels that insurers must notify in the event of a widespread incident. This would also allow insurers the ability to focus on restoration and minimizing harm to the consumer. Moving towards a standardized set of notification criteria and uniform notification expectations would greatly assist with this problem.

Conclusion

ACLI members recognize their affirmative obligation to maintain operations and protect consumer information amidst increasing cybersecurity threats. A united regulator and industry partnership is the best way to counter these threats. We encourage an ongoing dialogue between regulators and industry on cybersecurity issues to help both regulators and the industry better understand the other's underlying concerns, objectives, and challenges.

Thank you for your consideration of our comments. We welcome any questions.

Sincerely,

Kirsten Wolfford

Counsel, Cybersecurity Subcommittee Lead, ACLI

March 6, 2024

Cynthia Amann, Chair
Cybersecurity (H) Working Group
National Association of Insurance Commissioners

Re: Proposed Cybersecurity Event Response Plan

Dear Chair Amann:

The American Property Casualty Insurance Association (APCIA) welcomes the opportunity to comment on the Cybersecurity (E) Working Group's proposed Cybersecurity Event Response Plan (CERP). 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 members represent all sizes, structures, and regions—protecting families, communities, and businesses in the U.S. and across the globe.

APCIA continues to support the proposed CERP. However, for the sake of clarity, we believe the CERP should provide further detail regarding the information an insurer is expected to provide to a department of insurance (DOI) under item 5. Item 5 directs insurers to report, "the identity of the source of the cybersecurity event." We recommend adding more clarity regarding the type of information that the DOIs expect to receive pursuant to this item because it will be difficult for insurers to provide information about the source, and without more clarity, insurers will unlikely be able to provide usable information to the departments.

Thank you for considering the points addressed in this letter, and please do not hesitate to contact us if you have any questions.

Sincerely,

/s/ Casey McGraw

Casey McGraw
Vice-President of Policy & Counsel

cc: Sara Robben, srobben@naic.org
Miguel Romero, mromero@naic.org

NAMIC
NATIONAL ASSOCIATION OF MUTUAL INSURANCE COMPANIES

317.875.5250 | F 317.879.8408
3601 Vincennes Road, Indianapolis, Indiana 46268

202.628.1558 | F 202.628.1601
20 F Street N.W., Suite 510 | Washington, D.C. 20001

NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS
CYBERSECURITY (H) WORKING GROUP

CYBERSECURITY EVENT RESPONSE PLAN (CERP)
FEBRUARY 13, 2024 EXPOSURE DRAFT

MARCH 5, 2025

On behalf of the National Association of Mutual Insurance Companies (NAMIC)[1] members, thank you for the opportunity to provide these comments on the Cybersecurity Event Response Plan (CERP) exposure draft materials circulated on February 13, 2024. NAMIC offered previous input on May 1 and November 3, 2023. To the extent concerns raised there have not yet been addressed, we incorporate them here. While we thought that last year the Working Group determined that this document would be tested in draft form before being finalized, we understand that there has since been a decision to finalize and we appreciate many of the changes that have been made that help bring greater consistency.

NAMIC generally supports the idea of state regulators having ready a Cybersecurity Event Response Plan to establish expectations and to streamline the process. These comments are organized to discuss both the content of the exposure draft document and broader additional going forward considerations for the National Association of Insurance Commissioners (NAIC) and Departments of Insurance (DOIs).

Exposure Draft Document & Implementation

As the Working Group considers finalizing the CERP document, please consider how the draft might be amended to address the concerns outlined below.

Minimum Necessary Information: When requesting information, because of concerns with data security and privacy, state insurance regulators should restrict data requests to the minimum necessary to perform essential functions. In some cases, governmental bodies, such as DOIs, may have statutory exemptions from certain data privacy and security

[1] NAMIC Membership includes more than 1,500 member companies. The association supports regional and local mutual insurance companies on main streets across America and many of the country's largest national insurers. NAMIC member companies write $323 billion in annual premiums. Our members account for 67 percent of homeowners, 55 percent of automobile, and 32 percent of business insurance markets. Through our advocacy programs we promote public policy solutions that benefit NAMIC member companies and the policyholders they serve and foster greater understanding and recognition of the unique alignment of interests between management and policyholders of mutual companies.

legislation, potentially creating a less regulated environment with fewer controls to keep data safe. Unnecessarily transmitting or storing consumer data may therefore create undue risk to consumers. In addition, for broader protection of the insurance sector – given the nature of some of the vulnerability and remediation type information collected – data minimization is an important consideration. For these reasons, kindly consider adding a provision to the exposure draft (such as in the Understanding and Receiving Notifications and Required Information section) to indicate that DOIs should carefully consider each request for information and limit requests to the minimum necessary to perform its essential functions in order to minimize risks to consumers and to the insurance system overall.

Regulators Contacting Licensee's Outside Counsel or Third-Party Mitigation Firm: As currently drafted, CERP implies (in the second paragraph of the How to Receive Notifications and Acquire Required Information section) that a DOI may contact a licensee's counsel or third party mitigation firm directly. Without an agreement/request from the licensee, such direct engagement does not seem appropriate. Rather, by default, requests from the DOI should go to the regulated entity. Indeed, outside counsel may be prohibited from sharing information unless the licensee directs them to do so. Revising this paragraph could avoid misunderstandings and problems in the future.

Third-Party Service Providers: While the CERP draft acknowledges there are differences when dealing with a third-party service provider (in the Process for Responding to Cybersecurity Events section), it does not address the complexity sometimes presented by some scenarios. For example, consider the MOVEit situation in which there were multiple layers of third-parties reporting events at multiple layers. This created an environment where multiple insurers were attempting to obtain or provide the information from the providers to regulators and respond. To address this situation, the NAIC could explicitly define a process for aggregating and sharing information from the same third-parties because it could reduce the burden on both the insurers and the DOIs as it may lessen the number of requests and duplicative information. Addressing and streamlining such situations is a valuable opportunity for the NAIC and regulators to meaningfully improve the process and the system overall as well as to reduce the many moving parts to responding during an intense time of dealing with an incident.

Licensee Engagement Questions: Some questions a DOI may consider asking when making a determination of whether to engage the licensee are bulleted in the draft CERP (in the Process for Responding to Cyber Security Events section.) Please review a few suggestions. First, consider revising the law enforcement questions along the lines of "Is law enforcement aware of the licensee's situation? Does law enforcement appear to be involved?" Second, consider adding another question, consistent with some of the other themes highlighted in these comments, "Would engaging the licensee impact its ability to respond to the event?" Of course, it is important that the DOIs recognize the role and jurisdiction of law enforcement in post-event and the impact that may have on requests.

Event Notifications: There is some confusion around requirement in the CERP exposure draft (Understanding and Receiving Notifications and Required Information section) which states:

"Event notifications should be sent out promptly without waiting for all relevant information to be gathered." Could this be clarified? Without greater clarification, please consider deleting this sentence.

Early DOI-Licensee Communications: With respect to facilitating licensee notification to DOIs, as DOIs develop plans for cybersecurity events, it could reduce confusion and unnecessary back-and-forth if it were easier for licensees to determine who to contact at the Departments. Consider expanding the draft CERP (perhaps in the Forming a Team and Communicating with Consumers section) to indicate that the DOIs should post clearly on their websites to whom licensees should provide such notification. Similarly, it would be helpful for the CERP to clear that DOIs should endeavor to communicate with the lead named contact for the licensee as that may be more efficient and less confusing for those involved. This last point also relates to the concern about regulators contacting a licensee's outside counsel or third-party mitigation firm (discussed elsewhere in these comments).

Careful Communications with Law Enforcement & Other Regulators: If information is shared, it should only be done in a manner that will not subject the licensee (and/or the broader insurance system) to additional risk (e.g., cyber, litigation, additional inquiries that may distract from the response). Such protections could be outlined in the exposure draft (in the Communication with Law Enforcement and Other Regulators section).

Consistent Communications: If consumers receive duplicative and potentially different information, it may create confusion. To enhance consistency and to reduce potential confusion, the exposure draft (in the Forming a Team and Communicating with Consumers section) could include a suggestion that DOIs consider avoiding duplicative or inconsistent notifications to consumers (potentially referring consumers to the communications channels created and maintained by the licensee).

Sample Template: Several clarifications may be helpful in Appendix A. First, as a technical matter, consider whether the left column heading should read "Information Requested" rather than "Information Provided." Second, for row 9, additional clarification would be helpful beyond "this section." Third, for row 12, consider several small changes: "A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take / has taken to investigate and notify the consumers (as applicable) affected by the cybersecurity event."

Confidentiality & Trade Secret: There are several paragraphs (at the end of the Process for Responding to Cybersecurity Events section) that deal with protecting the information. Several suggestions have been offered to NAMIC. First, consider the following sentence: "If a licensee expresses concern about the sensitive nature of a particular document (for example, a forensics report), a DOI should consider performing a formal investigation pursuant to Section 7(A) of MDL-668." An alternative suggestion follows: "…a DOI should consider utilizing Section 7(A) of MDL-668 or other avenue allowing for confidentiality protections to a licensee." Second, at the end of that same paragraph, if the reference to limited-scope examination remains, consider inserting wording after it such as "(i.e., limited to compliance with the state's

version of MDL-668)…" Third, with respect to consulting legal counsel, one member suggests revising "must" to "may."

Trigger: Involvement by a DOI in the CERP should relate to an actual cybersecurity event in their state. Kindly consider referring to DOIs who received notice in accordance with Section 6 of MDL-668 (in the first paragraph of the Introduction).

DOI Review: While this CERP draft is much clearer around investigations and confidentiality, concern was raised to NAMIC (regarding the second paragraph on page 3 and within the Understanding and Receiving Notifications and Required Information section), about the prompting of a full scale investigation during time a licensee is responding to the cybersecurity event. Although reference is made to a "limited-scope investigation," please consider inserting an indication that care should be taken to minimize additional responses and investigation.

DOI Request Timing: As a technical item, in the paragraph following the bulleted questions (in the Process for Responding to Cybersecurity Events section), consider replacing "before stepping in " with "before seeking." (Another technical question several paragraphs down in the same section is whether "secured" should be "secure.")

Consistent Gathering As Much Required Information As Possible: A member suggests that the Working Group remove the word "consistently" from the CERP draft statement (in the Process for Responding to Cybersecurity Events section and based on the information after the comma in the sentence): "A DOI's process of responding to a licensee's cybersecurity event should allow it to consistently gather as much required information as possible without unduly burdening the licensee, and a DOI's engagement with the licensee may vary depending on the facts and circumstances of each cybersecurity event."

Uniformity & Implementation: The CERP is written to compliment model rule 668. As noted in the exposure draft (Scope section), states may adopt 668 as written, a revised version, or its own language—requiring states to modify the CERP. Thus, it is important to note, the CERP could be adopted in multiple forms across jurisdictions creating additional complexity, or conflicts, for insurers responding to an incident. NAMIC urges states to remain as near to uniform as possible to allow for reasonable consistency that would benefit both the regulators and the stakeholders when comes time to dealing with an actual cybersecurity event (and especially one impacting residents across multiple jurisdictions).

Additional Considerations

The February 13 email distributing the CERP exposure draft to interested parties stated that the Working Group decided to move away from a lead state approach and move toward studying one-to-many notification possibilities. NAMIC urges additional opportunities for stakeholders to engage on this topic, separate from the mention in the distribution of the updated CERP exposure draft.

At the highest level, NAMIC supports efforts to make cyber incident reporting and response more uniform. Efforts to streamline, standardize, and simplify the notification process – where licensees could reduce some of the communication channels and could focus on restoration – if implemented uniformly and carefully, could bring efficiencies that could be beneficial to both regulators and insurers.

At the same time, under a one-to-many approach, securing data robustly and avoiding vulnerabilities must be paramount. As the Working Group considers approaches, systems, and rules to govern such methods, careful consideration must be given to those protections and possible vulnerabilities (as well as to whether/how certain data fields are collected and stored in any central repository and distributed to certain states). Such considerations and protections are of utmost importance. Also, please consider the value of leadership via a lead state as a sufficient and helpful way to deal with more sensitive/vulnerable items/documents.

* * * * *

NAMIC would like to reiterate its ask to engage with the Cybersecurity (H) Working Group in an ongoing dialog with industry on efficiency (focusing on ways to improve consistency and streamline reporting) of cybersecurity reporting.

Thank you for your consideration of the concerns outlined in this statement and in those previously submitted by NAMIC on the CERP.

Discuss the Work Plan for the Working Group's Discussion on Cybersecurity and Cyber Insurance in 2024

Hear a Presentation from the Academy of Actuaries

Academy Cyber Presentation
NAIC 2024 Spring National Meeting

Richard Gibson, MAAA, FCAS

Senior Casualty Fellow, American Academy of Actuaries

American Academy of Actuaries

About the Academy

American Academy of Actuaries

The American Academy of Actuaries is a 20,000-member professional association whose mission is to serve the public and the U.S. actuarial profession. For more than 50 years, the Academy has assisted public policymakers on all levels by providing leadership, objective expertise, and actuarial advice on risk and financial security issues.

The Academy also sets qualification, practice, and professionalism standards for actuaries in the United States.

For more information, please visit:
www.actuary.org

The Academy's Vision & Mission

VISION: That financial security systems in the United States be sound and sustainable, and that actuaries be recognized as preeminent experts in risk and financial security.

MISSION: To serve the public and the United States actuarial profession.

American Academy of Actuaries

The Academy's Unique Purpose

- The Academy is the only U.S.-based actuarial organization solely focused on serving the public and the entire U.S. actuarial profession.
- It encompasses every practice area AND ensures the profession's ability to self-regulate, by housing the:
  - profession's standard-setting body, the Actuarial Standards Board;
  - profession's disciplinary body, the Actuarial Board for Counseling and Discipline;
  - Joint Committee on the Code of Professional Conduct; and
  - Committee on Qualifications.

The MAAA is recognized by legislators and regulators and referenced over 1,400 times in federal and state legislation and regulations.

American Academy of Actuaries

2023 Organizational Highlights

Membership

100+ CE credits
8K reached
40 webinars
3 seminars
1 annual meeting
1 Symposium

Education

300+

21 issue briefs
50 comment letters
6 practice notes
10 policy papers
105 presentations
10 podcasts
65+ articles
100 newsletters

Publications & Resources

Soc Sec Challenge
Student & Career Center
Credly Badge
New Member & Volunteer Webinars
10 exhibits
2.7M social reach
4.6K media hits
200K website visits
770K page views

Engagement & Awareness

American Academy of Actuaries

Academy Casualty Committees

- Casualty Practice Council (CPC) is the umbrella committee for major property/casualty issues.
- The CPC provides objective technical expertise to policymakers and regulators on major property/casualty issues, including medical professional liability and flood insurance.
- The Committee on Cyber Risk is one of 12 standing committees within the CPC.

American Academy of Actuaries

Committee on Cyber Risk

The Committee on Cyber Risk monitors the actuarial aspects of cyber risks.

Chairperson: Wanchin Chou, MAAA, FCAS

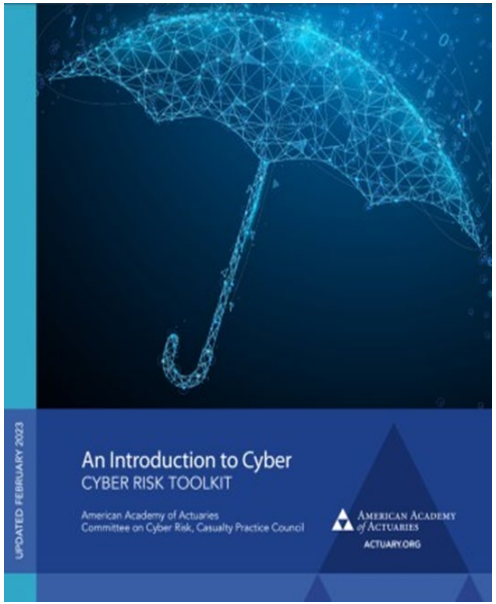
Vice Chairperson: Sam Tashima, MAAA, FCAS

More than 20 volunteer members on the committee

Cyber Risk Toolkit

The Cyber Risk Toolkit is a series of papers addressing issues pertinent to cyber risk insurance and cyber exposure.

actuary.org/cybertoolkit



American Academy of Actuaries

Cyber Risk Toolkit

- Developed by the Committee on Cyber Risk.
- Papers in the toolkit address issues pertinent to cyber risk and exposure which are now impacting most lines of business.
- Intended to be a resource for interested readers of the general public, public policymakers, the actuarial profession, the insurance sector, and other stakeholders.
- While each is a standalone paper, in total they offer a cohesive overview of the challenges posed in the cyber insurance market.
- The toolkit will continue to be updated periodically to reflect new and emerging work from the committee.

Cyber Risk Toolkit

An Introduction to Cyber

Cyber Threat Landscape

Silent Cyber

Cyber Data

Cyber Risk Accumulation

Cyber Risk Reinsurance Issues

Ransomware

War, Cyberterrorism, and Cyber Insurance

Autonomous Vehicles and Cyber Risk

Personal Cyber: An Intro to Risk Reduction and Mitigation Strategies

Digital Assets and Their Current Roles Within Cyber Crime

Cyber Risk Resource Guide

Upcoming topics:

Cyber Vendor Model Review

International Cyber Considerations

Personal Cyber Insurance Rating

American Academy of Actuaries

Additional Academy Cyber Research

Cyber Breach Reporting Requirements:
An Analysis of Laws Across the United States

Sponsored by the Committee on Cyber Risk and completed by Academy research staff (Nov. 2020)

Steve Jackson (Director of Research, Public Policy) is currently working with Prof. Marie Kratz of Essec Business School in Paris, France, to estimate the economic value of cyber risk, using an innovative method created by the professor, which takes into account both the heavy-tailed distribution of extreme events and the rapid changes in the underlying hazard.

Thank You!

For more information, please contact

Rich Gibson, Senior Casualty Fellow

gibson@actuary.org

Rob Fischer, Casualty Policy Analyst

fischer@actuary.org

American Academy of Actuaries

Hear a Presentation from CyberAcuView

CyberAcuView

NAIC Cybersecurity (H) Working Group
March 17, 2024

Mark Camillo, CEO

Monica Lindeen, Director of Regulatory Affairs

Mission

CyberAcuView aims to:

1. Help the industry provide **better value and service for policyholders** in their cyber risk mitigation
2. Provide leadership in **fighting cybercrime** and to **improve resilience** to cyber risk
3. Help ensure a **competitive market for cyber insurance**

CyberAcuView is industry-supported, working for the benefit of policyholders, the insurers that serve them, and the connected economy at large. All CyberAcuView activities are conducted consistent with antitrust best practices.

CyberAcuView is supported by the founding members which are major participants in the global cyber insurance market and include AIG, AXIS, Beazley, Chubb, The Hartford, Liberty Mutual Insurance, and Travelers.

Core Activities

CyberAcuView

1. **Data** aggregation, reporting, and standards
2. **Systemic risk** evaluation
3. **Regulatory** collaboration
4. **Law enforcement** coordination
5. **Other priorities** to improve market efficiencies

1. Data Aggregation, Reporting, and Standards

CyberAcuView

A. Data Aggregation

- Collect, validate, anonymize and aggregate data on policies, premiums and claims
- Create aggregated reports with value-added insights on the overall market
- Distribute data to members using a secure platform under antitrust monitoring

B. Statistical Reporting

- Enable industry members to retain value of their own data by becoming a statistical reporting agent
- Provide statistical reporting services in all states as required

C. Cyber Data Standards

- Developed an Incident Response Claims Taxonomy for both Cyber Exposure and Cyber Claims Data
- Publish standards as an Open Cyber Standard that is governed by CyberAcuView and can be accessed and used by all market participants

Highlights of Q3 2023 Data Call Results - US

CyberAcuView

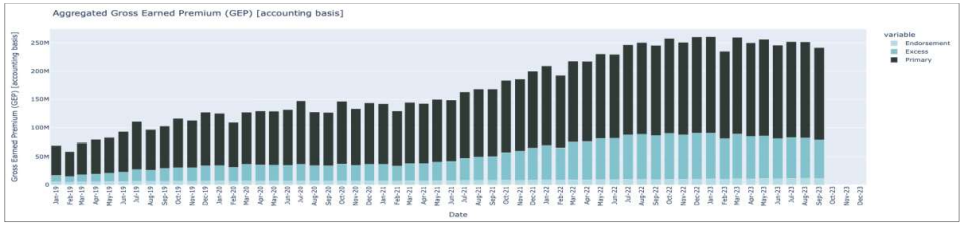
- Scope: 2019 – 2023 Q3
- Overall Data
  - Policies (4.2M policies collected): ≈$11B GWP and ≈$10B GEP
  - Claims Count: ≈30,000 claims
  - Losses Reported: ≈$4B paid and ≈$0.5B outstanding reserves
- Ransomware Claims
  - Claims Count: ≈9,000 claims
  - Losses Reported: $2.6B paid and $240M outstanding reserves

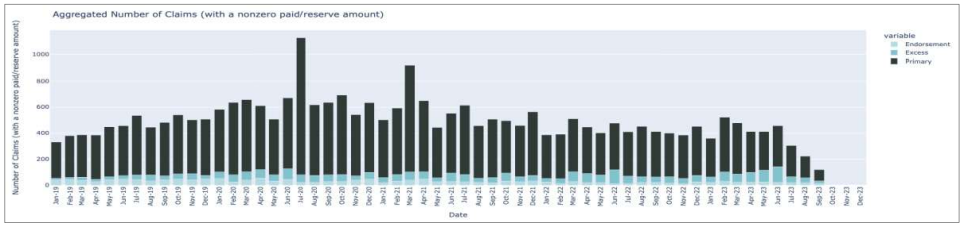
CyberAcuView Data Analytics - US

CyberAcuView

- High-quality, comprehensive data exhibits showcasing crucial metrics including premium, claim count, loss incurred, claims frequency, and claims severity.
- Multiple data dimensions, including analysis by time series, NAICS industry sector, revenue band, and policy type.
- Additional ransomware analysis, to provide insights into this rapidly evolving risk.

Example Exhibits from Data





Top 6 Ransomware Variants in terms of Ransomware Claims #

2023	2022	2021
BLACKCAT	BLACKCAT	CONTI
ROYAL	LOCKBIT 2.0	SODINOKIBI
LOCKBIT 3.0	HIVE	RYUK
BLACK BASTA	CONTI	LOCKBIT 2.0
LOCKBIT	PHOBOS	HIVE
CLOP	BLACK BASTA	PYSA

Top 6 Impacted Industry in terms of Ransomware Claims Loss Incurred $

2023	2022	2021
Retail Trade	Manufacturing	Prof., Sci., & Tech. Serv.
Manufacturing	Prof., Sci., & Tech. Serv.	Manufacturing
Accom. & Food Serv.	Health Care & Soc. Assist.	Health Care & Soc. Assist.
Prof., Sci., & Tech. Serv.	Retail Trade	Finance and Insurance
Finance and Insurance	Information	Retail Trade
Health Care & Soc. Assist.	Admin, Support, Waste Mgmt.	Wholesale Trade

2. Systemic Risk Evaluation

CyberAcuView runs quarterly workshops to stimulate discussion and help the industry:

- Develop a better **understanding of events** that drive systemic risk
- Discuss how the industry can **help address these areas**
- Help **increase society's resilience** to systemic cyber risk

Workshops have focused on:

- Cloud Failure/Outages
- Issues confronting the Cyber ILS/Alternative Capital Markets
- Systemic risk extensions that have been introduced in the marketplace
- Cyber risk modeling considerations

3. Regulatory Collaboration

CyberAcuView

CyberAcuView acts as a center of excellence that can lend its cyber expertise to other organizations working on cyber-related issues including:

- **National Association of Insurance Commissioners (NAIC) and State Regulators**
  - Foster strong working relationships with NAIC leadership, NAIC officers, key NAIC staff, and state regulators
  - Monitor and/or participate as necessary in NAIC committees, task forces, and working groups
- **Federal and International Regulators**
  - Federal Insurance Office (FIO)
  - CISA/DHS/ONCD
- **Other Organizations**
  - Insurance Trade Associations: APCIA, NAMIC, RAA, ABI, IUA
  - Technology and Security Companies
  - Other Consortium/Associations: Carnegie Endowment for International Peace (CEIP) US Chamber of Commerce, Center for Internet Security (CIS), etc.

Primary focus for 2024 will be on a potential backstop for catastrophic cyber events

Potential Backstop for Catastrophic Cyber

- In 2022, FIO released a Request for Comments on a Potential Federal Insurance Response to Catastrophic Cyber Incidents.
- In March 2023, the Administration publishes the National Cybersecurity Strategy, including Strategic Objective 3.6 stating that "The Administration will assess the need for and possible structures of a Federal insurance response to catastrophic cyber events that would support the existing cyber insurance market."
- In July 2023, the Administration published the Implementation Plan for the National Cybersecurity Strategy.

Potential Backstop (Continued)

CyberAcuView

- Initiative 3.6.1 designated Treasury as the responsible agency, stating:
  - *"Assess the need for a Federal insurance response to a catastrophic cyber event,"*
  - *"The Department of Treasury's Federal Insurance Office, in coordination with CISA and ONCD, will assess the need for a Federal Insurance response to catastrophic cyber events that would support the existing cyber insurance market".*
- Public meeting/conferences were held in UC Irvine and NYU in 2023
- A third conference is scheduled for early May 2024

4. Law Enforcement Coordination

CyberAcuView

CyberAcuView aims to strengthen relationships between the insurance industry and law enforcement to help address the increasing threats of cyber-attack, through:

- Establishing **relationships with the FBI, Interpol, and others** who are responsible for responding to the cyber threat.
- Leveraging these relationships to create robust **cyber risk information sharing** opportunities
- Collecting and distributing critical information to bring value to the public and private sector in the **fight against cybercrime**

Developing a pilot program to actively disrupt and seize ransomware payments by coordinating with other technology companies

5. Other Priorities

CyberAcuView

- Developed a **CyberAcuView policy form** that can be used by market participants to define risks more precisely, remove ambiguities, and to attract more capacity into the market. The cyber war exclusion language was accepted and posted to the LMA website.
- Endorsed voluntary **minimum cyber security best practices** to improve policyholder cyber security maturity
- Expanded **CyberAcuView's role outside of the US** with first international data call in the UK and Canada
- Collaborated with PERILS to create a **U.S. Cyber Loss Index** to help accelerate the growth of the Cyber-ILS and ILW markets

Update on Cyber Loss Index

- PERILS AG and CyberAcuView entered into a cooperation agreement to provide a cyber industry loss reporting service covering U.S. primary market losses.
- CyberAcuView identifies and designates events based on Widespread Event language in the CyberAcuView policy form
- CyberAcuView collects the estimated ultimate gross loss from each Data Provider and then extrapolates the aggregated losses based on the percentage of total US gross written premium
- Only cyber insurance industry losses above $500M are reported
- Ultimate losses are updated quarterly up to three years following an event end date.
- More details on the methodology can be found at https://cyber.perils.org/#/methodology

Discuss Any Other Matters Brought Before the Working Group