Draft: 11/16/2022

Cybersecurity (H) Working Group
Virtual Meeting
November 15, 2022

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met Nov. 15, 2022. The following Working Group members participated: Cynthia Amann, Co-Chair (MO); Wendy Erdly, Co-Chair (NY); C.J. Metcalf, Co-Vice Chair (IL); Michael Peterson, Co-Vice Chair (VA); Sian Ng-Ashcraft (AK); Chris Erwin (AR); Lance Hirano (HI); Alex Borkowski (MD); Jake Martin (MI); Troy Smith (MO); Martin Swanson (NE); Colton Schulz and Chris Aufenthie (ND); Barbara D. Richardson (NV); Don Layson (OH); Dan Petterson (VT); John Jacobson (WA); and Rachel Cissne Carabell (WI).

1. Adopted its October 11 Meeting Minutes

Schulz made a motion, seconded by Amann to adopt the Working Group's October 11 minutes (Attachment Three-A). The motion passed unanimously.

2. Discussed Cybersecurity with the Cybersecurity and Infrastructure Security Agency (CISA)

Erdly led a discussion with CISA's Executive Director, Brandon Wales. The discussion touched on several topics.

Wales said that CISA's work consists of two broad missions. CISA is responsibility for coordinating national efforts around critical infrastructure, security, and resilience. Because CISA is not a part of the law enforcement community or the intelligence community, the organization is purpose built for partnership with industry. The second mission is related to operational responsibility for the security of federal, civilian executive branch networks. CISA provides information, guidance, and technical advisories related to cybersecurity.

Related to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), Erdly asked about the act, what makes it important, and how CIRCIA will determine who is critical infrastructure and therefore will be subject to the reporting requirements of the Act. Wales responded that CIRCIA will help the federal government have better visibility to cybersecurity trends noting that currently the federal government estimates that it only knows about 20 to 30% of the cyber attacks that hit the United States which prevents the government from providing early warning to additional victims which further allows campaigns to spread more quickly. Therefore the law now requires incident reporting with CISA working on what will qualify as a covered incident who will qualify as a covered entity. CISA wants to make sure that when they issue their final rule to apply the authority given to them in CIRCIA, that result in a clear definition allowing members of industry to understand whether they qualify as critical infrastructure or not. Lastly, CISA also wants to make sure that they are receiving the most relevant information for covered incidents understanding that incidents evolve quickly and that limited information may be available at times. Erdly asked further about the type of information CISA anticipates gathering with Wales responding that the information will be of the sort that helps CISA advise the rest of the community about emerging threats including information on tactics and techniques used by adversaries. Erdly asked if the incident information CISA gathers could be shared with state insurance regulators. Wales responded that there are restrictions in how information can be used, for instance criminal proceedings, and so there may be information they have to remove for privacy reasons, but that CISA anticipates being able to share information with state insurance regulators. Miguel Romero (NAIC) asked if CISA anticipated taking an active aiding in the investigation of cybersecurity incidents or passive role largely focused on gathering information. Wales responded that CISA's role can vary based on what is needed but that generally they expect to gather information when working with

industry representatives. Romero asked if the information gathered would include consumer level information. Wales responded that given CISA's focus on protecting all companies, consumer level information may not be relevant.

Erdly next asked about CISA's Cybersecurity Performance Goals. Erdly indicated that the goals originate from a National Security Memorandum signed by President Biden on July 2021. The memorandum required that CISA work with the National Institute of Standards of Technology (NIST) to develop baseline cybersecurity performance goals that are consistent across all critical infrastructure. The goals are a voluntary set of cybersecurity practices intended to help those deemed to be critical infrastructure, especially small and medium sized organizations. Wales added that the goals were developed with industry input and that the goals are a focused set of controls most essential to achieving positive cybersecurity outcomes. They draw on the NIST Cybersecurity Framework (CSF), but don't cover every practice referenced in the CSF. The goals also include insights on the anticipated cost and complexity of implementation so organizations can evaluate their own capacity as they decide which controls to implement.

Erdly next asked how state insurance regulators can support CISA's work. Wales talked about the importance of having sound due diligence related to cybersecurity insurance underwriting because he views cyber insurance as a really critical mechanism to improve cybersecurity risk mitigation. Wales further indicated that the Department of Treasury is studying at the possibility of a federal backstop for cyber insurance.

Erdly next asked about CISA's Shield's Up Program. Wales indicated that the program originated in 2021 as the US government recognized that Russia was likely to invade Ukraine and that there may be implications for US cybersecurity based on the US's support for Ukraine. The program recommends a series of steps a company should take to mitigate risk possibly as a reprisal from Russia. Suggested practices include using multi-factor authentication on administrative accounts and segmenting networks as much as possible. The program also suggests other practices for instance lowering the threshold for reporting incidents to governmental agencies and making sure the company has adequate equipment for operations in case of supply chain issues.

3. Discussed Other Matters

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

Https://naiconline.sharepoint.com/sites/NAICSupportStaffHub/Member Meetings/H CMTE/2022_Fall/Cybersecurity/C(H)WG 11-15-2022 Minutes.docx

The Cybersecurity (H) Working Group 2023 Workplan:

Working Group Charges:

A. Monitor cybersecurity trends such as vulnerabilities, risk management, governance practices and breaches with the potential to affect the insurance industry.
B. Interact with and support state insurance departments responding to insurance industry cybersecurity events.
C. Promote communication across state insurance departments regarding cybersecurity risks and events.
D. Oversee the development of a regulatory cybersecurity response guidance document to assist state insurance regulators in the investigation of insurance cyber events.
E. Monitor federal and international activities on efforts to manage and evaluate cybersecurity risk.
F. Coordinate NAIC committee cybersecurity work including cybersecurity guidance developed by the Market Conduct Examination Guidelines (D) Working Group and the Information Technology Examination (E) Working Group.
G. Advise on the development of cybersecurity training for state insurance regulators.
H. Work with the Center for Insurance Policy and Research (CIPR) to analyze publicly available cybersecurity related information.
I. Support the states with implementation efforts related to the adoption of *Insurance Data Security Model Law* (#668).

- Workstream 1: Cybersecurity Response Plan

Subject Matter Expert Group Lead: Cindy Amann/Michael Peterson

Summary: Regulators will develop an optional guide to assist states in responding to cybersecurity events among their regulated entities. The project will include, but is not limited to:

- A Review of existing regulator cybersecurity response plans
- Drafting an outline of main topics to be included in the cybersecurity response plan to ensure the necessary topics are incorporated into the response plan
- Drafting a response plan
- Creating a reporting template to aid states in collecting information in the wake of a cybersecurity event

Timeline: Completed by 2023

Related Charges: This project would fall under charges B, C, and D.

Considerations: Regulators should consider:

- Whether the response plan should include a reporting template
- Whether the publication should be a public or regulator only resource

- Workstream 2: Referral to the Information Technology (IT) Examination (E) Working Group (ITEWG)

Subject Matter Expert Group Lead: N/A

Summary: Referral should be sent by Summer NM, but the actual underlying project may last until 2024 depending on the approach chosen by ITEWG

- Update the Financial Examination Handbook to strengthen and update guidance for financial examiners to draw on more focus on cyber during an exam.

Related Charges: This project would fall under charge E.

Considerations: The Working Group needs to recognize that there is overlapping membership between the ITEWG and the Cybersecurity (H) Working Group, limiting the Working Group's resources.

- Workstream 3: Training

Summary: The Working Group could work with NAIC staff, regulators, and industry to identify cybersecurity subject matter that warrant training. The Working Group would oversee the development of training.

The Working Group could also work with D/E committee groups to aid in the identification of relevant certifications/credentials that Departments of Insurance could use to help in developing subject matter expertise.

Timeline: The working group could develop an initial plan by the Summer National Meeting and thereafter, the work would transition to an ongoing project.

Related Charges: This project falls primarily under charge F but the training material may relate to other charges.

Considerations: While there are many topics that may warrant training, resource limitations will make it important to prioritize training requests considering the significance/prevalence/complexity of said subject matter.

H Committee and other related groups may also undertake related efforts. Work should be coordinated to avoid duplication of effort.

- Workstream 4: Monitoring

Subject Matter Expert Group Lead: Wendy Erdly

Summary: The Working Group has several charges that relate to monitoring and coordination. At rotating meetings, regulators could receive updates from NAIC staff or regulators:

- Cybersecurity trends
    - Industry may also assist in the identification of relevant trends
- The relevant work done at the Market Conduct Examination Guidelines (D) Working Group and the Information Technology Examination (E) Working Group
- State efforts to implement/adopt the *Insurance Data Security Model Law* (#668)
- The relevant work done at federal and/or international level

Timeline: The working group should consider engaging in some monitoring effort on an annual basis, but otherwise, there is no expiration or timeline for this work.

Related Charges: This project would fall under charges A, C, and D.

Considerations: With each item discussed, it would be relevant to consider whether the Working Group should take action. Actions would be determined based on the situation. It's most likely that federal/international work would lead to such action/responses.

NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

MEMORANDUM

TO: Jerry Ehlers, Chair, Information Technology (IT) Examination (E) Working Group
Ber Vang, Vice-Chair, Information Technology (IT) Examination (E) Working Group

FROM: Cindy Amann, Co-Chair, Cybersecurity (H) Working Group
Wendy Erldy, Co-Chair, Cybersecurity (H) Working Group
CJ Metcalf, Co-Vice-Chair, Cybersecurity (H) Working Group
Michael Peterson, Co-Vice-Chair, Cybersecurity (H) Working Group

DATE: March 7, 2023

RE: Cybersecurity Procedures

The Cybersecurity (H) Working Group has several charges that call on the working group to monitor industry trends and to coordinate our work with the IT Examination (E) Working Group. Those include:

A. Monitor cybersecurity trends such as vulnerabilities, risk management, governance practices, and breaches with the potential to affect the insurance industry.
E. Monitor federal and international activities on cybersecurity engaging on efforts to manage and evaluate cybersecurity risk.
F. Coordinate NAIC committee cybersecurity work, including cybersecurity guidance developed by the Market Conduct Examination Guidelines (D) Working Group and the Information Technology (IT) Examination (E) Working Group.

In keeping with those charges, the Cybersecurity (H) Working Group met with the Executive Director from the Cybersecurity and Infrastructure Security Agency (CISA), Brandon Wales, who provided an update on his agency's work. As part of the update, Mr. Wales mentioned his agency's work to develop and publish a "Cross-Sector Baseline Cybersecurity Performance Goals (CPGs)". Per CISA's website, "the CPGs are a prioritized subset of IT and operational technology (OT) cybersecurity practices that critical infrastructure owners and operators can implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques."

More importantly, these CPG's the Cybersecurity (H) Working Group is suggesting this publication to the IT Examination (E) Working Group as it may represent an opportunity to update the cybersecurity related guidance contained within the *Financial Condition Examiners Handbook* (Handbook). While the guidance in the Handbook has long served regulators as an effective tool to investigate a myriad of risks, cybersecurity included, this tool or other resources may represent an opportunity to ensure the work program appropriately prioritizes cybersecurity related considerations.

Therefore, the Cybersecurity (H) Working Group asks the IT Examination (E) Working Group to consider the following:

- Whether the existing guidance would benefit from an update to better prioritize cybersecurity risks.
- If so, whether the CPGs or a different resource (i.e., NIST, CIS, etc.) would aid in a project to update cybersecurity guidance.
    - For instance, the CIS listing of security controls includes a tiering that may make that a useful tool that allows regulators to distinguish relevant controls from key controls.
- Whether any international developments could prove beneficial as a resource towards this project (i.e., Issues Paper under development by the Operational Resilience Task Force).

This is potentially a substantial project, but one that could enhance the regulatory ability to investigate cybersecurity risks. An update may also identify specific procedures that are less relevant as the focus of investigations prioritizes cybersecurity over the review of IT general controls. Upon a quick review by one of our Working Group volunteers, we found substantial overlap between the CPGs and the existing Handbook work program. However, the IT Examination (E) Working Group may find that the CPGs more clearly or simply articulate the controls that are needed to directly address cybersecurity risks. There may also be procedures that while still relevant could be de-emphasized or investigated via inquiry to better allow for cybersecurity to remain a core focus.

The Cybersecurity (H) Working Group acknowledges less ambitious ideas may also be appropriate but stands ready to support the work of the IT Examination (E) Working Group in whatever approach to this project and study is chosen.

Please work with our NAIC support staff, Miguel Romero and Sara Robben to keep our group updated on your progress and decisions.

OUTLINE FOR INCIDENT RESPONSE FOLLOWING A CYBERSECURITY EVENT
CYBERSECURITY (H) WORKING GROUP

I. Introduction

Paragraph defining the purpose of the response plan, considerations when choosing a response team, sections the plan will cover.

II. Communication with other States/Federal Regulators

This section should include examples of when a state needs to reach out to other states or to federal regulators.

III. Initial Notification by Domestic

This section should discuss a means for the licensee to report an incident. This section could suggest the various methods of reporting.

IV. Meetings

The number of meetings will be determined once the depth of the cybersecurity incident is determined; however, an initial meeting should be set up so the response team at the DOI to learn about the event, reports regarding contacting law enforcement, and to determine if follow-up meetings are needed.

V. Communication with the Firm Handling the Incident

This section should include details received from the firm handling the incident regarding the details of the incident, as well as the steps taken to remediate the incident and notify affected consumers.

VI. Organizational Security

This section should contain details of Organizational security, including, but not limited to: Training, logical security, operational security, physical security, network security, application security, and vulnerability assessment.

VII. Risk Assessment

This section should provide a description of how the licensee assesses risk. Example could be how a company assesses risk of third-party vendors and software, use of a third-party to assess cyber resilience, including but not limited to table-top exercises.

VIII. Audits

This section should include any policy or program audits.

IX. Communication with Consumer

This section should include information that should be communicated to a consumer following a breach.

X. Summary of Regulator Tools

XI. Coordination of Communication

XII. Information Gathering Template

This section should include the types of information that are important to gather following a cybersecurity incident.

