Draft: 3/16/2023

Cybersecurity (H) Working Group
Virtual Meeting (*in lieu of meeting at the 2023 Spring National Meeting*)
March 7, 2023

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met March 7, 2023. The following Working Group members participated: Cynthia Amann, Co-Chair (MO); C.J. Metcalf, Co-Vice Chair (IL); Michael Peterson, Co-Vice Chair (VA); Julia Jette (AK); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Shane Mead (KS); Matt Kilgallen (GA); Daniel Mathis (IA); Alexander Borkowski (MD); T.J. Patton (MN); Jake Martin (MI); Troy Smith (MT); Colton Schulz and Chris Aufenthie (ND); Martin Swanson (NE); David Bettencourt (NH); Justin Herrings (NY); Matt Walsh (OH); John Haworth (WA); and Rebecca Rebholz (WI).

1. Adopted its 2022 Fall National Meeting Minutes

Haworth made a motion, seconded by Schulz, to adopt the Working Group's Nov. 15, 2022, minutes (*see NAIC Proceedings – Fall 2022, Innovation, Cybersecurity, and Technology, Attachment* Three). The motion passed unanimously.

2. Discussed its Work Plan for 2023

Amann summarized the Working Group's work plan for 2023 (Attachment A) The work plan contains four components, called workstreams, building from the results of the Working Group's survey to state insurance regulators in 2022.

The first item on the work plan is to develop a cybersecurity response plan. The subject matter expert (SME) group leads for this workstream are Amann and Peterson. The outline for the response plan includes 12 topics to date:

- Introduction
- Communication with other states/federal regulators
- Initial notification by domestic
- Meetings (initial and follow-up meetings if necessary)
- Communication with the firm handling the incident
- Organizational security
- Risk assessment
- Audits
- Communications with consumers
- Summary of regulator tools
- Coordination of communication
- Information-gathering template

A drafting group is being formed, and drafting will begin following the Spring National Meeting.

The second item on the work plan is for the Working Group to send a referral to the Information Technology (IT) Examination (E) Working Group asking it to consider updating its cybersecurity guidance (Attachment B).

The third item on the work plan is for the Working Group to continue to support NAIC training initiatives. This workstream will identify cybersecurity subject matters. The Working Group will work with NAIC staff, state insurance regulators, and the insurance industry to identify warranted training. Any work considered by this workstream requires coordination with the Innovation, Cybersecurity, and Technology (H) Committee to avoid duplications of effort.

The fourth item on the work plan is for the Working Group to continue to monitor cybersecurity trends among regulated entities and among federal and international bodies. State insurance regulators will receive relevant updates regarding cybersecurity trends, work being completed by related working groups, state efforts to adopt the *Insurance Data Security Model Law* (#668), and relevant work happening at the federal and international levels.

Amann concluded by asking states to consider volunteering and contacting NAIC staff with their specific interest in supporting components of the work plan. Romero noted that workstream one, the cybersecurity response plan, is the workstream most likely to need assistance. Romero acknowledged past willingness to aid from Connecticut and North Dakota.

Haworth asked if the Working Group would meet in regulator-to-regulator session to discuss cybersecurity events. Amann said there may be a case for regulator-only sessions for some of the issues the Working Group will be addressing. Romero indicated that if there is a specific subject matter related to an examination or another confidential matter, a regulator-only meeting would be a possibility.

3. Heard an Overview of the Treasury Department's Report Titled *The Financial Services Sector's Adoption of Cloud Services*

Ethan Sonnichsen (NAIC) provided an overview of the U.S. Department of Treasury's (Treasury Department's) *The Report on the Financial Services Sector's Adoption of Cloud Services*, which was released on Feb. 8. The report discusses the benefits and challenges of the financial services sector's increasing adoption of cloud services technology. It also makes several recommendations for financial service providers and the regulatory community.

The report summarizes some of the benefits, including scalability, cost savings, and the security of the information technology infrastructure. In the financial services sector, there is a concentration among a small number of cloud service providers. Risks may involve a significant system failure or data breach at a large cloud service provider, which may have substantial implications for the financial services sector and the customers they serve. Many financial services institutions additionally expressed concerns regarding a cloud service provider's (CSP's) cybersecurity vulnerabilities. Currently, there is a lack of data in the financial regulatory community regarding the number of providers and the types of services provided at CSPs.

The report addressed concerns from institutions regarding the lack of transparency of reporting, as several of the institutions surveyed noted they do not receive information regarding incidents, outages, or other problems at the CSP that would affect the institution's system or its customer's access to information.

The report highlights a talent gap at financial services firms, including training expertise and the ability to determine which services to transition to a cloud infrastructure. The talent gap is the most pressing issue for smaller institutions.

The report also notes there is exposure to potential operational incidents at CSPs. Many financial services institutions additionally expressed concerns regarding CSPs' cybersecurity vulnerabilities or a service failure. Financial service regulators need more data regarding a financial institution's exposures.

Additionally, the report addresses the global regulatory requirements and how those may create challenges for firms wishing to migrate to a cloud service. There are regulatory differences around the world, making it difficult for a large global financial institution wanting to transition to the cloud. Some countries have restrictive data policies requiring data to be housed locally, whereas the U.S. is less restrictive regarding data flows.

Likewise, the report addresses concerns regarding market concentration. First, the market is concentrated among a small number of CSPs; third-parties may also use the same CSP. This concentration means an incident has a better chance of spreading throughout the financial system. Market concentration exists across banking, securities, and insurance markets. There is also a need to close significant data gaps regarding a financial institution's use of a CSP to better understand its risk exposure.

The report asks financial institutions to think about building a communication plan with its CSP, establishing a risk management framework to prioritize which systems will move to the cloud, whether there are backups and controls to execute them, and to introduce performance metrics showing the financial institution is receiving some economic value by transitioning to the cloud.

A cloud services steering group will be created in the next year or so to focus closer on domestic collaboration among financial regulators regarding cloud services. The steering group will consider writing best practices for cloud adoption and cloud contracts to provide some standardization. Interagency collaboration and coordination will be important. The steering group will also examine the data gap regarding CSP usage and determine what the financial regulators need to know regarding the reliance at a CSP.

The steering group will also look at protocols for incident response and engaging on international standards as the international standard setting groups, as well as fostering some industry discussions to obtain a direct account of what is happening in the financial services sector as cloud standards are adopted.

Amann asked the Working Group to consider the data state insurance regulators need, why they need it, and what the data will disclose regarding an insurer's use of cloud service providers. She asked the Working Group to also think about how this data is best obtained, whether the data is confidential data, unidentified data, group data, individual insurer data, how frequently the data needs to be collected, and if there are exemptions.

Peterson said that he believes the Treasury Department intends to remain active on this topic. He suggested that state insurance regulators could take the initiative to create a solution that works for both insurers and state insurance regulators. Peterson proposed that state insurance regulators use the systems summary grid, a tool in the *Financial Condition Examiners Handbook*, to help gather information on insurers' industry-wide use of cloud service providers. He suggested that a regulator-only filing submission could be beneficial as a new annual filing and would help regulators from a macroprudential perspective of an insurers' cloud service usage. There would be logistics to work through, including whether template standardization is necessary. Peterson asked the Working Group to consider whether this is a viable path forward to help state insurance regulators gather cloud service provider information.

Romero restated the proposal regarding whether regulators could use the systems summary grid to streamline the transmission of information on an insurer's use of cloud service providers, including whether data is needed and how frequently data needs to be submitted. Amann emphasized the need for insurers' input on this proposal. Romero indicated that given the time left for the meeting, the Working Group could solicit industry input on this proposal via e-mail following the meeting. Upon receiving the insurer's input, the Working Group could reconvene to continue the discussion.

4. Discussed a Referral to the IT Examination (E) Working Group.

Amann said that because of the discussion last year with the Cybersecurity and Infrastructure Security Agency (CISA), the Working Group will be asking the IT Examination (E) Working Group to consider updating its cybersecurity-related guidance based on the CISA cybersecurity performance goals. Romero indicated that the Working Group has a charge to monitor and not to update cybersecurity guidance. Therefore, the referral sends the matter to the Working Group, having authority over cybersecurity guidance.

The Working Group's referral acknowledges there may be resources apart from the CISA cybersecurity performance goals. Updated guidance could help ensure the addressing of cybersecurity-related risks.

Brian de Vallance (Center for Internet Security—CIS) stated that cybersecurity is an important topic for state insurance regulators to consider and that the CIS supports updating the guidance as cyber defense has evolved. He noted that the CIS would be available to assist state insurance regulators as they continue to study this project.

5. Discussed the Outline for the Incident Response Plan

Amann stated that the Working Group's charge of creating an incident response plan builds on the Model #668 and would aid the states in requesting information from insurers that have experienced a cybersecurity event.

Amann indicated that insurers' input benefits this project, specifically in addressing the type of information that would be available. Romero indicated that in following up with states regarding the state insurance regulators' needs, the survey identified the demand for a tool assisting states in responding to cybersecurity events among regulated entities. Such a tool would help guide states in the communication and information-gathering responsibilities of the department of insurance (DOI). The tool would enhance a state's ability to act as a lead state in a cybersecurity event and minimize state inquiries to regulated entities.

States could tailor the tool to suit their individual needs. Romero suggested the Working Group form a drafting group to advance the tool's planning and suggested creating an information-gathering template and the value therein from an insurer's perspective.

Peter Kochenburger (University of Connecticut School of Law) said consumer representatives might also provide valuable input to ensure consumer notifications are included in the response plan. Schulz suggested that the workstream leverage insights from past NAIC cybersecurity tabletop exercises to assist with this project.

6. Discussed Other Matters

Skyler Gunther (NAIC) said that the NAIC would lead an effort to facilitate vendor presentations from Security Scorecard and Bitsight to provide information to state insurance regulators regarding cyber-risk analytic capabilities. Herring indicated that the New York Department of Financial Services (DFS) has been using Security Scorecard and may provide beneficial information in the Working Group's consideration of these tools. Romero indicated that after the vendor meetings, the state insurance regulators would reconvene to consider the usefulness of these tools.

