INNOVATION, CYBERSECURITY, AND TECHNOLOGY (H) COMMITTEE

Innovation, Cybersecurity, and Technology (H) Committee Nov. 19, 2024, Minutes
- Big Data and Artificial Intelligence (H) Working Group Nov. 17, 2024, Minutes (Attachment One)
  - Big Data and Artificial Intelligence (H) Working Group Nov. 12, 2024, Minutes (Attachment One-A)
- Privacy Protections (H) Working Group Nov. 17, 2024, Minutes (Attachment Two)
- Cybersecurity (H) Working Group Nov. 18, 2024, Minutes (Attachment Three)
  - Cybersecurity (H) Working Group Oct. 30, 2024, Minutes (Attachment Three-A)
  - Cybersecurity (H) Working Group Oct. 8, 2024, Minutes (Attachment Three-A1)
  - Cybersecurity (H) Working Group Sept. 4, 2024, Minutes (Attachment Three-A1a)
    - Cybersecurity (H) Working Group Aug. 1, 2024, Minutes (Attachment Three-A1a1)
      - Cybersecurity (H) Working Group May 29, 2024, Minutes (Attachment Three-A1a2)
- 2025 Proposed Charges (Attachment Four)

Draft Pending Adoption

Draft: 12/4/24

Innovation, Cybersecurity, and Technology (H) Committee
Denver, Colorado
November 19, 2024

The Innovation, Cybersecurity, and Technology (H) Committee met in Denver, CO, Nov. 19, 2024. The following Committee members participated: Kevin Gaffney, Chair, and Rosemary Raszka (VT); Michael Conway, Co-Vice Chair (CO); Chlora Lindley-Myers, Co-Vice Chair, represented by Cynthia Amann (MO); Ricardo Lara represented by Ken Allen (CA); Karima M. Woods represented by Sharon Shipp (DC); Michael Yaworsky represented by Anoush Brangaccio (FL); Gordon I. Ito represented by Jerry Bump (HI); Ann Gillespie (IL); Marie Grant (MD); Jon Godfread and John Arnold (ND); Judith L. French represented by Daniel Bradford (OH); and Michael Humphreys and Shannen Logue (PA). Also participating were: Wanchin Chou and George Bradner (CT); Jake Martin (MI); Angela Hatchell (NC); Christian Citarella (NH); Elizabeth Kelleher Dwyer (RI); Cassie Brown (TX); and Scott A. White and Michael Peterson (VA).

1. Adopted its Summer National Meeting Minutes

Commissioner Conway made a motion, seconded by Commissioner Humphreys, to adopt the Committee's Aug. 15 (*see NAIC Proceedings – Summer 2024, Innovation, Cybersecurity, and Technology (H) Committee*) minutes. The motion passed unanimously.

2. Adopted the Reports of its Working Groups

A. Data Call Study Group

Commissioner Godfread provided a presentation and an overview of the plans for the Data Call Study Group. The group will help regulators obtain more detailed and higher-quality data. In 2025, the group will review the three primary NAIC data collection systems from 2024 to identify challenges insurers face with data calls, including the Financial Data Repository (FDR), Market Conduct Annual Statement (MCAS), and regulatory data collections (RDC).

Commissioner Godfread said that improving the data call processes will help address data needs while minimizing the need for ad-hoc data calls. In phase 1 of the work, regulators will work with NAIC staff to conduct detailed inventories of data definitions and data called/stored by the NAIC with a later transition to receiving presentations from insurer representatives. The phase 1 membership will include regulators, drawing from across the NAIC's areas of expertise. In the later stages of phase 1, the group will broaden its membership, inviting more regulators to join and industry representatives as well.

In phase 2, the group will engineer solutions, assess staffing impact, train and support regulators, and transition to implementation. In phase 3, regulators will establish a data governance framework to address the process for revising the data model, data definition ownership, data update cadences, and data collection methods and will encourage feedback from stakeholders in identifying potential enhancements and innovations.

Peter Kochenburger (NAIC Consumer Representative) thanked Commissioner Godfread for his presentation and work on big data and AI but said he believes regulators should move on from discussing data definitions and urged regulators not to merely continue with years of study and education. Nancy Clark (Verisk) mentioned that her company has been working with regulators and data standardization to improve access and tools, and she asked to be included as conversations progress. Clark said that her group has been working on a tool that she has shown to several meeting attendees that shows what Verisk is looking to have available to regulators to assist in their data calls.

B. Privacy Protections (H) Working Group

Director Dwyer discussed the Privacy Protections (H) Working Group's ongoing work to expose the chair draft of the *Privacy of Consumer Financial and Health Information Regulation* (#672) section by section. The Working Group went through the third-party section of Model #672 in two open meetings and then discussed the section further during a regulator-only meeting. The section was later released to the public but not through a formal comment period, allowing the public to see the document before it is exposed with a full comment period after more progress is made on the draft. The Working Group is currently working on Article 3, which includes four sections. Comments have been requested by Nov. 25. This is not a full 30-day comment period because there will be a longer comment period for the completed draft. This is to avoid prolonging the drafting process with repeated and extended comment periods.

Commissioner Godfread made a motion, seconded by Commissioner Conway, to adopt the Privacy Protection (H) Working Group's request to extend the deadline for completion of Model #672 until December 2025. The motion passed unanimously.

Commissioner Godfread thanked NAIC staff supporting this work, including Holly Weatherford, Jennifer Neuerburg, and Lois Alexander.

C. Cybersecurity (H) Working Group

Amann reported that the Cybersecurity (H) Working Group met Oct. 30, Oct. 8, and Sept. 4, Aug. 1, and May 29 to discuss the development of a cybersecurity event response notice portal that would allow regulators to centrally receive cybersecurity event responses that regulated entities submit in response to an event. This portal would be housed and maintained by the NAIC within its robust security environment. She said there are many discussions to be had on the topic, but the Working Group has had great engagement with regulators and the public about this idea. During the Working Group's Nov. 18 meeting, regulators adopted a motion to authorize the group to work with the NAIC to explore the creation of the portal. Amann asked that if the Committee has input, the Working Group would incorporate the feedback.

Acting Director Gillespie made a motion, seconded by Commissioner Conway, to adopt the report of the Big Data and Artificial Intelligence (H) Working Group (Attachment One), Privacy Protections (H) Working Group (Attachment Two) and Cybersecurity (H) Working Group (Attachment Three). The motion passed unanimously.

3. Adopted its 2025 Proposed Charges

Commissioner Gaffney said that since the charges were initially distributed, the posted document has been corrected, as the charges document had an extra data study group charge under the Big Data and Artificial Intelligence (H) Working Group. The data study group charge should fall under the H Committee only. Additionally, the SupTech/GovTech Roundtable is now listed as a Subgroup instead of a Roundtable to align with the NAIC's group naming conventions.

Commissioner Gaffney said regulators are shifting toward taking some additional steps to advance artificial intelligence (AI) discussions. Accordingly, to manage workloads, the Committee is disbanding two groups: the Technology, Innovation, and InsurTech (H) Working Group and the E-Commerce (H) Working Group. Commissioner Gaffney thanked the leaders of these groups.

Sarah Wood (Insurance Retirement Institute—IRI) commented that she hopes the industry will have the opportunity to raise matters previously given to the E-Commerce (H) Working Group as needs arise.

Amann made a motion, seconded by Commissioner Conway, to adopt the Committee's 2025 proposed charges (Attachment Four). The motion passed unanimously.

4. Heard a Presentation from FireBreak Risk on the Use of AI to Help Mitigate Wildfire Risk

Kate Stillwell (FireBreak Risk) discussed the concept of ember cast, a phenomenon responsible for 90% of home loss, according to firefighters. Ember cast is the occurrence of embers flying ahead of a fire, and home hardening attempts to address this phenomenon.

Stillwell showed an example of how various fence types impact house fires, which is further supported by academic research. Fire-hardened homes are 40% more likely to survive even if only partially hardened, according to researchers from the University of British Columbia and the University of California San Diego.

FireBreak Risk assists insurers by providing data to identify mitigated homes which supports mitigation discounts and offers insurance in previously uninsurable areas. Stillwell noted that many home hardening details can only be seen from an on-the-ground view which requires self-inspection given the scale of inspections needed. While some home hardening assessments can be viewed aerially or via satellite, many home hardening details, such as the wood under a deck or mesh on vents, cannot be seen via those mechanisms.

FireBreak Risk provides a self-inspection application that policyholders use to help them understand the most significant mitigation actions, and many of them can be done directly by the policyholder with relative ease. The application is AI-powered and helps compile data based on images of property attributes which insurers and policyholders can use to assess and mitigate risk. FireBreak Risk uses a combination of vendor AI models and internally developed models. Its technology can detect and categorize objects, rank risk level, and suggest images of features that could help reduce risk.

Property attributes are rated on a four-tier scale (poor, good, better, best). Working with insurers, FireBreak Risk maps attribute according to building standards to help assess risk. The company is an early-stage startup, but insurers are already using its models to mitigate risk. Stillwell closed by expressing a desire to work with regulators to strengthen the availability of insurance and protect consumers.

Commissioner Gaffney asked if FireBreak Risk has learned any lessons as they have developed and deployed its technology. He asked if any of the attributes that are considered change as part of the development process, for example. Stillwell said they learned that perfect cannot be the enemy of good. Insurance underwriters need to understand that compliance with home building standards can be difficult but that encouraging risk mitigation, even if gradual, can be meaningful. She also explained that carriers are not always prepared to assess every property attribute, but they do use the overall assessment rating to determine if homeowners and their property meet or exceed standards. FireBreak Risk initially thought that risk selection and underwriting profitability would drive insurer adoption, and then it realized that customer engagement is driving the company's business, as the application allows insurers to interact with policyholders in a beneficial way leading to better engagement and increased use of the application.

Chou discussed the many wildfire modelers and asked if FireBreak Risk has worked with modelers to see if the modeler's data on risk is consistent with FireBreak's view of risk. Stillwell said that FireBreak Risk has engaged with modelers, including CoreLogic, to understand how FireBreak's data adapts and modifies when used by underwriters. FireBreak Risk looks for similar engagement with other modelers as well.

Bradner asked how Firebreak Risk verifies continued compliance in the assessed properties. Stillwell said that insurers drive that decision, and FireBreak recommends that insurers require a reinspection at the time of renewal and before the start of wildfire season, as many property attributes change over the course of the year. Bradner asked if there were plans to work on a flood-related application. Stillwell said that it would not be in 2025 until clients raise interest.

5. Heard a Presentation from InsurTech Coalition Members on the Responsible Use of AI

Jennifer Crutchfield (Clearcover) said that Clearcover is a private passenger auto (PPA) carrier operating in 19 states as a fully licensed insurance carrier that is also expanding to include a reciprocal exchange structure.

Crutchfield played a video showing the power of AI via its TerranceBot application, which the company refers to as Terry. The application helps claims representatives and adjusters through the claims process. Terry can summarize a claim, answer specific questions about a claim, and help draft correspondence with customers.

The company also has customer-facing generative AI capabilities through the recent launch of "DiSCoBot," which is short for Digital Statement Collection. Claims representatives sometimes need to collect extensive information, and DiSCoBot helps to automate the information-gathering process. DiSCoBot mimics the judgment of a claims representative and asks tailored questions as the process proceeds.

Before consumers interact with DiSCoBot, consumers are informed the application is AI-based and are given the opportunity to opt in. Clearcover reports a 73% opt-in rate. Clearcover works with a third party to test DiSCoBot for bias in addition to the company's own testing and monitoring. The company monitors for hallucination rates, robotic responses, and correct exit criteria among other attributes. The company also monitors for shifts or drifts in the model response. Crutchfield closed by saying that Clearcover understands that AI is a powerful tool and is committed to incorporating consumer feedback and improving transparency to build a trusted relationship with both consumers and regulators.

Scott Fischer (Lemonade) presented on Lemonade's AI governance. Fischer said that Lemonade started developing a governance framework by working with Tulsee Doshi, who was formerly with Google, and involves a cross-disciplinary group of employees including data scientists and compliance-oriented professionals.

The governance framework discussion started with a recognition that AI represents a new and more powerful suite of tools even beyond generalized linear models, allowing companies to assess and use data in new and complex ways, creating the need to operate with great responsibility. He said the governance framework is built to provide every user with equal opportunity and to lead the industry as a trusted insurance partner. Lemonade designed its framework to ensure consumers with similar risk profiles get similar access to products and the opportunity to claim losses, and it ensures that models adhere to policies and are held accountable. The framework was based on the National Institute of Standards and Technology (NIST) Framework.

Lemonade has an AI responsibility committee with broad and senior representatives from across the company, including the parent company's CEO. This committee establishes guidelines and principles, advises and reports to the company's board of directors, and oversees the company's AI working group, which implements what the AI responsibility committee has approved.

A key tenant of the framework includes a clear definition of what is in scope and, thus, what counts as a model. At Lemonade, the definition of a model includes models that are broader than intended in Lemonade's interpretation of the NAIC's *Model Bulletin on the Use of Artificial Intelligence Systems by Insurers*. Lemonade's governance starts by categorizing data into high, medium, and low sensitivity tiers. High-sensitivity data includes protected class information. Low-sensitivity data includes attributes of insured items or data that are easily

verifiable with medium-sensitivity data. These categorizations drive the degree of oversight for each model. High-sensitivity models typically are those that impact a customer's ability to access insurance or claims. Low-sensitivity models predict attributes of pets or properties. Medium-sensitivity models are models with humans in the loop and include any model with telematics. Fischer said he believes all of this structure aligns well with Section 3 of the NAIC's model bulletin.

Lemonade has a model governance process that consists of a model governance checklist that calls on the company to explain the model, its data, intended uses, and other key pieces of information. The company has also created model cards to nimbly explain each model by describing the purpose and treatment, data sampled, features used, performance, and key figures specific to each model.

Commissioner Gaffney thanked the presenters and said he appreciated the comparison of their governance framework to the NAIC's model bulletin. Director Richardson asked Crutchfield about Clearcover's view of acceptable hallucination rates. Crutchfield said that Clearcover does not have an acceptable hallucination rate with even one hallucination causing a pause in the use of a given model. Crutchfield said that hallucinations occurred in training but have not occurred frequently since training.

Peterson asked about the human-in-the-loop concept and how Lemonade decides when to involve humans. Fischer said the decision is based on the use of risk and the sensitivity of the model. If the model is focused on verifying facts, such as dog breed and roof age, the need for a human may be less as opposed to a model related to claims. The assessment is based on the impact on consumers. Miguel Romero (NAIC) asked how Lemonade developed a metric threshold for any of the cited examples (hallucination rates, robotic response, correctness criteria, etc.). Crutchfield said she would have to get back to the Committee after consultation with the company's data scientists, but she knows a flag is raised with every instance related to the criteria. Fischer added that he would like the actuarial community to advance the discussion in setting objective thresholds for industry best practices. For instance, the New York State Department of Financial Services has issued a circular letter that calls for a disparate impact standard, but it is unclear what the specific threshold would be. Romero asked about the design of the model cards and decisions on what information to include. Fischer said that the company learned from best practices of other tech companies and drew on publicly available information in consultation with Doshi.

Having no further business, the Innovation, Cybersecurity, and Technology (H) Committee adjourned.

SharePoint/NAIC Support Staff Hub/Member Meetings/H CMTE/2024_Fall/H-Minutes/Minutes-H-Cmte111924-Final.docx

Draft: 12/3/24

Big Data and Artificial Intelligence (H) Working Group
Denver, Colorado
November 17, 2024

The Big Data and Artificial Intelligence (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Denver, CO, on Nov. 17, 2024. The following Working Group members participated: Michael Humphreys, Chair, and Shannen Logue (PA); Doug Ommen, Co-Vice Chair (IA); Kevin Gaffney, Co-Vice Chair, and Mary Block (VT); Sian Ng-Ashcraft and Molly Nollette (AK); Richard Fiore (AL); Tom Zuppan (AZ); Ken Allen (CA); Michael Conway and Jason Lapham (CO); Wanchin Chou (CT); Karima M. Woods and Dana Sheppard (DC); Richie Frederick (FL); Shannon Hohl (ID); Julie Rachford and Joanna Coll (IL); Holly W. Lambert and Victoria Hastings (IN); Shawn Boggs (KY); Tom Travis (LA); Caleb Huntington and Jackie Horigan (MA); Kory Boone (MD); Sandra Darby (ME); Jeff Hayden (MI); Phil Vigliaturo (MN); Chlora Lindley-Myers and Cynthia Amann (MO); Colton Schulz and John Arnold (ND); Connie Van Slyke (NE); Christian Citarella (NH); Seong-min Eom (NJ); Hermoliva Abejar (NV); Matt Walsh (OH); Teresa Green (OK); Raven Collins (OR); Karl Bitzky (SC); Travis Jordan (SD); Emily Marsh (TN); J'ne Byckovski and Cassie Brown (TX); Michael Peterson (VA); Jay Bruns (WA); Tim Cornelius (WI); Juanita Wimmer (WV); and Lela Ladd (WY). Also participating was Melissa Robertson (NM).

1. Adopted its Nov. 12 Minutes

Commissioner Ommen made a motion, seconded by Commissioner Gaffney, to adopt the Working Group's Nov. 12 minutes (Attachment One-A). The motion passed unanimously.

2. Received an Update on the Health AI/ML Survey

Commissioner Humphreys stated that the health AI/ML survey workstream has held weekly discussions for the past year to set the scope of the health artificial intelligence (AI)/machine learning (ML) survey, refine questions, and incorporate input, and clarified that the Working Group is not conducting the survey, rather the participating group of states is doing research to assist the Big Data and Artificial Intelligence (H) Working Group. Commissioner Humphreys reiterated that the goals of the surveys were to: 1) gain a better understanding of the insurance industry's use and governance of AI; 2) seek information that could aid in the development of guidance or potential regulatory framework to support the insurance industry's use of AI; and 3) inform regulators of the current and planned business practices of companies. On Oct. 31, the call letter to the surveyed companies was issued. On Nov. 11, the surveys were launched with a due date of Jan. 22, 2025. By March 17, the responses will be compiled, and the report of the findings is targeted to be published on March 24.

Logue reported that, in response to consumer representative feedback, the main differences between the health AI/ML survey and prior AI/ML surveys included: 1) individually tailoring questions to different product lines (comprehensive individual major medical plans, comprehensive small employer major medical plans, comprehensive other [i.e. large] employer major medical plans, and individual and group student health plans) and 2) tailoring the questions to the areas of data usage, arrangements with third parties, coordination of governance with existing health provider governance standards, and the different operational AI functions of health insurers.

3. Received an Update on the Follow-Up to the PPA AI/ML Survey

Logue stated that the purpose of the follow-ups to the private passenger auto (PPA) surveys was to compare the current state of AI usage in 2024 with the baseline from the 2021 surveys. Follow-up discussions are being held with a subset of companies that responded to the 2021 surveys to gather updates on the companies' approach to AI since the 2021 survey. The types of questions asked during the follow-up meetings included if the NAIC *Model Bulletin on the Use of Algorithms, Predictive Models, and Artificial Intelligence Systems by Insurers* has been helpful, if the carrier has established a governance program, and if testing is performed and the extent of it, including testing of third-party-provided AI systems. The follow-up surveys will take place through the first quarter of 2025.

4. Heard a Presentation on Health Insurance Companies' Use of AI to Conduct Utilization Management

Lucy Culp (Leukemia & Lymphoma Society—LLS) and Lauren Seno (NORC at the University of Chicago—NORC) summarized the comprehensive report "Artificial Intelligence in Health Insurance: The Use and Regulation of AI in Utilization Management," focusing on prior authorization. The report was a collaborative effort between NORC and the LLS and provided an in-depth analysis of AI's current implementation and potential implications for health care services. Culp and Seno highlighted both promising opportunities and significant concerns surrounding AI's role in health care decision-making. While AI technologies offer potential benefits, such as reducing administrative burden, expediting approval processes, and allowing health care professionals to focus on more complex clinical tasks, i.e., to practice "at the top of their license," there are concerns about current limitations and potential risks, including inherent bias in training data about the historical underrepresentation of marginalized and minoritized communities in health care data sets and significant gaps in clinical data. They noted that many demographic groups have been systematically excluded from clinical trials and claims data, and these data limitations could potentially perpetuate existing health care inequities.

Culp and Seno emphasized the risk of misaligned incentives, where AI systems might prioritize cost containment over patient care, and the potential for AI algorithms to evolve beyond their original intended usage, creating challenges for regulation and oversight. In response to these challenges, the report proposed a comprehensive regulatory framework consisting of three pillars: 1) meaningful transparency; 2) accountability mechanisms; and 3) robust human oversight. It was noted that current regulatory efforts are limited, with only a few states (California, Colorado, and Utah) actively developing comprehensive AI regulations for health insurance processes, suggesting that technological implementation is significantly outpacing the development of regulatory frameworks. They stated that regulation is a way to bring alignment between the use of AI with how society expects them to function.

Culp and Seno noted that a critical recommendation in the report was the development of governance structures that can effectively measure and prevent potential harm to historically marginalized communities, stressing the importance of ongoing monitoring, testing, and refining of AI systems to align their functionality with societal expectations. They concluded by emphasizing that human oversight is important. Robust and accessible appeals processes for coverage denials need to be established and considered a guaranteed right for all health insurance consumers. Human oversight must be embedded into underwriting management when AI is used, and those reviewers must have the authority and ability to overturn decisions made by the AI without undue consequences. AI regulation needs to be considered an evolving practice.

Commissioner Humphreys asked the presenters when transparency should be provided to the consumer and in what form it would be most helpful. The presenters responded that, in particular, consumers should be informed

whether they are interacting with an AI tool and in cases where prior authorization is denied. They added that transparency disclosures should follow a risk-based approach.

Horigan asked whether changes should be made to the appeals process. The presenters responded that it should be based on accountability behind the AI system and that the process should be clarified when an AI tool is involved.

Boone asked whether insurance companies are indicating that they want proper safeguards on a granular level or on a higher level. The presenters responded that the goal is not to stifle innovation but to make sure that consumers are protected. Innovation that can have positive impacts should be encouraged while accountability should be established for when there is not always a positive impact.

Commissioner Gaffney asked the presenters to comment on how to better assess the input data. The presenters responded that health care data is understood through claims data, but that only captures what happened and what was paid for. There is so much care that is not happening for systemic reasons that does not get captured in that data, so thinking beyond claims data is a potential start. Other approaches are truing up data sets and auditing input training data sets to ensure the data is representative.

5. Heard a Presentation on Use Case Applications of AI in Insurance Underwriting and Claims

Frank Quan (University of Illinois) presented AI use cases in insurance underwriting and claim management, noting that these two areas are the most impactful on consumers. Quan first highlighted that recent advancements in generative AI can replicate institutional knowledge to help streamline the underwriting process and improve the customer experience by using external data to prefill policyholder information, drastically reducing the number of questions the consumer needs to answer during the submission process. However, Quan noted that this may raise important questions about how to ensure accuracy, how consumers can correct errors, how consumers can dispute unfair outcomes, and what transparency disclosures should be made to consumers.

As another example, Quan highlighted how AI can be used in claims management, where AI-powered systems can automatically review and process claims by analyzing claim documentation, images, and historical data, in order to prioritize suspicious claims to be routed to humans within a special investigations unit. He noted that AI models may have many submodels to handle the variety of data, such as computer vision models, large language models, and supervised learning models. These systems require continuous monitoring and regular data audits. For example, most insurers do not have sufficient loss experience for Tesla Cybertrucks, resulting in possibly inaccurate estimates of damage predictions. AI systems require a careful balance between automation and human oversight, transparent algorithm development, and a strong commitment to ensuring data quality. Regarding regulatory compliance, the focus should be whether the model is targeting certain demographic groups unfairly.

Further, Quan noted that AI systems can also be exploited by fraud actors who analyze which claims are likely to be approved and adjust their claim submissions to fit the preferred patterns. This can undermine automated processes, so insurers need fraud detection models. One of the challenges in creating a fraud detection system is sampling from a biased or unrepresentative data set. Another challenge is that fraud detection models may generate high rates of false positives and false negatives, potentially resulting in an unfair outcome.

Chou asked whether Quan has had the chance to do a cost-benefit analysis of using AI in underwriting and claims, and the relationship between a third-party actor, the lawyer, and the doctor in fraudulent claims. Quan responded that on the first question, he has not worked at an insurance company, so therefore, he does not have access to

the data needed to do a cost/benefit analysis. On the second question, it is very difficult to identify fraud claims and relationships among acting parties because of the very low number of actual fraud claims available in historic training data.

Horigan asked whether there should be AI model pushback on some human-in-the-loop decisions if the model perceives that the human is making biased decisions. Quan responded that AI is just a replication of human beings, and if humans are already biased, then the model must be biased, so there is no way an AI system can correct human beings based on historically biased information. One way to correct this is from the data inputs perspective, and the other way is to correct this from the output level.

6. Discussed its 2025 Proposed Charges

Commissioner Humphreys noted that the charge "Overseeing the Work of the Data Call Study Group" will be addressed by the H Committee, not the Big Data and Artificial Intelligence (H) Working Group. The inclusion was an error, and he apologized for any confusion.

Commissioner Humphreys said the Working Group is taking steps to advance the discussion on what comes next, as the group adopted the AI principles in 2020. The *Model Bulletin on the Use of Artificial Intelligence Systems by Insurers* was adopted last year, and 19 states have adopted it. He said that each adoption was an important milestone in the Working Group's path to updating the regulatory framework for the use of AI.

He said the two items that the Working Group will begin to work on will be a discussion with Commissioner Ommen on AI systems evaluation which he explained during the Working Group's Nov. 12 meeting. Commissioner Humphreys said the Working Group has additional charges that shift the overall discussions to consumer outcomes, i.e., what does the Working Group want to protect the consumer from? He clarified that the Working Group understands AI is a transformative technology that many are using beneficially, and this may lead to a gap analysis. He said that once the Working Group has specified what it wants to protect consumers from, it will have to decide if its framework holds up against those potential harms. He said that there will be more discussion to come, and he looks forward to the group's engagement.

Having no further business, the Big Data and Artificial Intelligence (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Fall/WG-BDAI/Fall-Minutes/Minutes-BDAIWG111724.docx

Draft: 11/19/24

Big Data and Artificial Intelligence (H) Working Group
Virtual Meeting
November 12, 2024

The Big Data and Artificial Intelligence (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met Nov. 12, 2024. The following Working Group members participated: Michael Humphreys, Chair, and Shannen Logue (PA); Kevin Gaffney, Co-Vice Chair, and Mary Block (VT); Doug Ommen, Co-Vice Chair (IA); Alex Romero and Molly Nollette (AK); Jimmy Gunn (AL); Tom Zuppan (AZ); Ken Allen (CA); Jason Lapham (CO); George Bradner (CT); Karima M. Woods (DC); Rebecca Smid (FL); Weston Trexler (ID); C.J. Metcalf (IL); Victoria Hastings (IN); Tom Travis (LA); Caleb Huntington (MA); Kory Boone (MD); Sandra Darby (ME); Jeff Hayden and Jake Martin (MI); Phil Vigliaturo (MN); Cynthia Amann and Brad Gerling (MO); Tracy Biehn (NC); Colton Schulz (ND); Megan VanAusdall (NE); Christian Citarella (NH); Scott Kipper (NV); Kevin Yan (NY); Matt Walsh (OH); Matt Gendron (RI); Andreea Savu (SC); Vickie Trice (TN); J'ne Byckovski (TX); Michael Peterson (VA); Eric Slavich (WA); Nathan Houdek (WI); Juanita Wimmer (WV); and Lela Ladd (WY).

1. Adopted its July 29 Meeting Minutes

Darby made a motion, seconded by Commissioner Gaffney, to adopt the Working Group's July 29 meeting minutes (*see NAIC Proceedings – Summer 2024, Innovation, Cybersecurity, and Technology (H) Committee*). The motion passed unanimously.

2. Heard a Presentation on How AI Is Used in Insurance Including Implementation Challenges and Lessons Learned

Tom Prince (Milliman) began the presentation by providing background on artificial intelligence (AI) in insurance, emphasizing the rapid pace of change and the need for the insurance industry to respond to the rise of AI. He noted that while the insurance industry is well-positioned to leverage AI given its quantitative foundation, there are still major challenges to overcome. He discussed several use cases including developing chatbots and assistants for tasks like legal compliance, actuarial guidance, and rate/product filing. The key lessons from these efforts include the difficulty of getting these systems to be fully reliable and trustworthy, as retrieval augmented generation (RAG) and human oversight are critical, as well as the importance of using the most advanced foundational AI models available and the need for close collaboration between technology teams and domain experts to effectively leverage AI capabilities.

Prince discussed the risks associated with generative AI, highlighting areas of data security/privacy, bias, and risks to the human-AI configuration within organizations. He referenced a National Institute of Standards and Technology (NIST) framework for managing these AI risks and noted the alignment to the NAIC's *Model Bulletin on the Use of Artificial Intelligence Systems by Insurers*. However, he noted the importance of going beyond having a structured framework that, while useful and necessary, is not sufficient. Rather, a careful assessment must be taken to prioritize and take action in proportion to the level of risk.

Gendron asked whether sufficient research has been done on the importance of process controls and whether synthetic data could be used to test for potentially illegal or inappropriate outcomes. Prince responded that there are some process controls in ratemaking, such as using hold-out data for testing and testing the impacts of individual variables in modeling, but he has not seen much research about using synthetic data to test for illegal or inappropriate outcomes.

Prince closed by briefly mentioning that the use of third-party AI systems comes with the risk of vendors being acquired or becoming bankrupt. Commissioner Humphreys acknowledged that the Third-Party Data and Models (H) Task Force will examine those issues.

3. Received an Update on the AI Systems Evaluation Workstream

Commissioner Ommen provided an update on the AI systems evaluation workstream's efforts, stating that following up on the adoption of the model bulletin, the workstream has had several discussions to determine the next steps in order to help regulators on the use of AI. Commissioner Ommen stated that one initiative the NAIC took was forming the Third-Party Data and Models (H) Task Force this year, with the goal of establishing an effective framework to regulate the use of AI systems sourced from third parties. Another initiative is to begin discussions on AI systems evaluations, which was initially started as a collaboration forum but is now working under and in coordination with the Big Data and Artificial Intelligence (H) Working Group, as new charges are being considered by the H Committee. This work will help regulators update the regulatory framework to help assess the effectiveness of insurer AI governance programs and risk mitigation strategies as laid out in the expectations in the bulletin.

The AI Systems Evaluation workstream was formed to help regulators ask the right questions and provide guidelines and tools to help evaluate the potential for risk that might arise from the use of AI systems. Commissioner Ommen noted that this workstream has started by looking at what has already been developed in the Big Data and Artificial Intelligence (H) Working Group and other working groups such as the Accelerated Underwriting (A) Working Group and its guidance in automated life insurance underwriting, and the Casualty Actuarial and Statistical (C) Task Force and its *Regulatory Review of Predictive Models* white paper. The workstream also has been discussing what new tools need to be developed to help assess the extent to which AI is being used, where and how to assess potential risk, and then assess an insurer's governance program.

Commissioner Ommen reviewed the drafted charges for the workstream, which are: 1) identify existing tools, resources, materials, and training that will assist and guide regulators in their review of AI systems used by licensees, including an insurer's AI program which includes establishing a coordinated work plan and timeline for further development of those resources; 2) develop new regulatory tools or regulatory guidance to assist regulators in their review of AI systems used by licensees, including an insurer's AI program; and 3) coordinate the development of review and enforcement tools, resources, guidelines, and training related to AI systems for regulators across the NAIC.

Commissioner Ommen reiterated that in the short term, the workstream is looking into the initial tools, resources, and education necessary to meet the immediate needs of enforcing the bulletin and assessing the use and risks of AI, but in the longer term, the workstream will be continuing to have discussions about how an overall AI regulatory framework should be developed and possibly incorporated into the *Market Regulation Handbook* or whether it is more appropriate to establish a stand-alone handbook. Commissioner Ommen noted that as a possible timeline, in the remaining time this year, the workstream will continue to review AI evaluation work from other NAIC groups and will determine the need to develop tools for regulators to help assess how AI is used by an insurance company. Then, in 2025, the workstream will discuss the market regulation process and recommend updates to the D Committee, and in 2026, it will support the implementation of proposals to update regulations and/or establish new regulations to address how AI is used in the industry.

Peter Kochenburger (Southern University Law Center) commented that the materials presented by the AI Systems Evaluation workstream do not include mention of consumer rights and that disclosure requirements are not the solution to data privacy. He then asked when the NAIC will turn to addressing specific consumer rights.

Commissioner Humphreys responded by stating that a couple of consumer representatives will give a presentation to the Big Data and Artificial Intelligence (H) Working Group at the upcoming Fall National Meeting, and the Working Group anticipates hearing from consumers to help identify the most appropriate way to regulate the use of AI in insurance. Commissioner Humphreys further noted that the AI/machine learning (ML) surveys brought to light how the industry is using AI today, and while the NAIC has issued initial guidance in terms of general principles, the idea has always been to pursue the next steps to develop a comprehensive plan to move forward to regulate the use of AI in insurance.

Commissioner Gaffney added that the states are still in the process of adopting the bulletin, and at the same time, the Working Group is communicating its voice in a lot of different venues about the expectations of the bulletin. The AI Systems Evaluation process is looking to possibly add procedures to the *Market Regulation Handbook* and will have consumer protections in mind. The NAIC will remain transparent, and it welcomes continued input from consumer groups.

Having no further business, the Big Data and Artificial Intelligence (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Member Meetings//H CMTE/2024_Fall/WG-BDAI/2024 1112Interim-Meeting\Minutes-BDAIWG-111224.docx

Draft: 12/3/24

Privacy Protections (H) Working Group
Denver, Colorado
November 17, 2024

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Denver, CO, Nov. 17, 2024. The following Working Group members participated: Elizabeth Kelleher Dwyer, Chair (RI); Ann Gillespie, Co-Vice Chair (IL); Victoria Hastings, Co-Vice Chair (IN); Chelsy Maller (AK); Richard Fiore (AL); Gio Espinosa and Catherine O'Neil (AZ); Damon Diederich and Jennifer Bender (CA); George Bradner and Kristin Fabian (CT); Doug Ommen and Johanna Nagel (IA); Van Dorsey (MD); Robert Wake and Stacy Bergendahl (ME); Jeff Hayden (MI); T.J. Patton (MN); Cynthia Amann (MO); Molly Plummer (MT); Santana Edison (ND); Martin Swanson (NE); Raven Collins (OR); Michael Humphreys, Jodi Frantz and Richard Hendrickson (PA); Frank Marnell (SD); Katie Johnson and Dan Bumpus (VA); Todd Dixon (WA); Lauren Van Buren (WI); Bryan Stevens (WY). Also participating was Matt Gendron (RI).

1. Adopted its Summer National Meeting Minutes

Director Dwyer reported that the Working Group met Nov. 4 in regulator-to-regulator session, pursuant to paragraph 6 (consultations with NAIC staff members related to NAIC technical guidance) of the NAIC Policy Statement on Open Meetings. It also met in open session Oct. 31 and Sept. 30. During these meetings, the Working Group took the following action: 1) discussed Section 5—Third Party Arrangements of the chair draft revising the *Privacy Consumer Financial and Health Information Regulation* (Model #672), with a focus on Subsection 5A(6); heard comments from interested parties on Section 5 of Model #672; and 3) discussed its next steps.

Following these meetings, the Working Group exposed Article III, Sections 6, 7, and 8 of the chair draft revising Model #672 for a public comment period ending Nov. 25. Director Dwyer reported that the Working Group will hold an open meeting to discuss comments on Article III in December.

Director Dwyer also addressed a request from several trade groups to extend the comment deadline to Dec. 6. Director Dwyer said the Working Group would not be extending the deadline for comments because the chair draft was released Aug. 5, and the public had ample time to review the draft and compile comments. The Working Group wants to keep making progress and, therefore, cannot dedicate 30-day comment periods for each section.

Frank Marnell made a motion, seconded by Victoria Hastings, to adopt the Working Group's Aug. 14 (*see NAIC Proceedings – Summer 2024, Innovation, Cybersecurity, and Technology (H) Committee*) minutes. The motion passed unanimously.

2. Approved Extension of Time to Draft Revisions to the *Privacy of Consumer Financial and Health Information Regulation* (#672)

Director Dwyer noted that the Working Group would like to request an extension to continue drafting revisions to Model #672.

Director Gillespie made a motion, seconded by Damon Diederich, to extend the time to draft revisions to Model #672. The motion passed unanimously.

3. Heard an Update on Federal Privacy Legislation

Shana Oppenheim (NAIC) reported that the Consumer Financial Protection Bureau (CFPB) released a landmark regulation restricting how financial institutions handle consumer information in a bid to set rules for banks and fintechs on data access. The long-awaited rule, which aims to make it easier for consumers to switch banks and requires greater data security from fintechs, is an attempt to level the playing field between rival businesses and give people more control over their own information. The rule requires companies to heed customers' requests to share information with other businesses offering competing products, and banks will be required to make personal financial data freely available to consumers. Companies that access a person's data will not be able to use it for targeted advertising, and consumers must reauthorize access to their data annually, with the right to revoke access at any time.

The CFPB will also work on additional guidance and advisory opinions to advance open banking and payments. The CFPB said it will also look for opportunities for other types of financial data, such as those involving investments and securities in retirement plans, to plug into this ecosystem.

Next, Ms. Oppenheim stated that the American Privacy Rights Act of 2024 (APRA) would establish national consumer data privacy rights and set standards for data security. She said it mandates transparency from covered entities on data usage and grants consumers rights to access, correct, delete, and export their data. Consumers can also opt out of targeted advertising and data transfers. The APRA enforces data minimization, allowing data collection only for necessary purposes, and prohibits transferring sensitive data without explicit consent. Enforcement will be handled by the Federal Trade Commission (FTC), state attorneys general, and consumers.

The APRA was introduced by U.S. House of Representatives (House) Energy and Commerce Committee Chair Rep. Cathy McMorris Rodgers (R-WA) and Senate Commerce Chair Sen. Maria Cantwell (D-WA). A new version faced pushback from Grand Old Party (GOP) leadership, tech lobby, and privacy advocates, leading to a canceled markup with no rescheduled timeline. Opposition to the APRA includes law enforcement groups, the Interactive Advertising Bureau (IAB), United for Privacy, and the Main Street Privacy Coalition, citing concerns over data deletion, targeted advertising, preemption, and private right of action.

The APRA applies to entities under the FTC Act, including nonprofits, with exemptions for small businesses under certain conditions. It covers all individuals, treating minors' data as sensitive. Covered data includes identifiable information, excluding de-identified data and publicly available information. Sensitive data encompasses categories like race, health, and biometric information. The Act emphasizes data minimization and purpose limitation, requiring clear purposes for data collection. Large data holders must conduct Privacy Impact Assessments (PIAs). The Act also mandates privacy and data security officers for covered entities, with additional requirements for large data holders. The Act allows a private right of action for violations, with the potential for class action lawsuits. It preempts non-sectoral state privacy laws but preserves certain state law provisions related to employee, student, and health privacy.

New sections in the APRA 2.0 include the Children's Online Privacy Protection Act (COPPA) 2.0, Privacy by Design, expanded public research purposes, and obligations for data brokers. Changes to algorithmic impact assessments and consequential decision opt-out are also included. The Act aims to create a uniform national data privacy standard while preserving specific state law rights.

The bill faces opposition moving forward, so it is not expected to move forward at this time.

4. Heard a Presentation on Privacy Principles Proposed by NAIC Consumer Representatives

Harry Ting (Health Care Consumer Advocate) stated that the privacy principles focus on licensee obligations and are not intended to be model law wording or to restrict the ability to prevent criminal activity, fraud, material misrepresentation, nondisclosure, or limit state regulators' ability to protect consumers' nonpublic personal information.

Dr. Ting also detailed the first two privacy principles: 1) you have the primary responsibility to protect the consumer nonpublic personal information (NPI) you collect; and 2) only ask the consumer for NPI needed to fulfill the consumer's business with you or to fulfill legal obligations.

Eric Ellsworth (Consumers' Checkbook and Center for the Study of Services—CSS) reported on privacy principles three through five: 3) only collect nonpublic personal information that you can protect with concrete policies and procedures that state insurance regulators can review; 4) only transfer nonpublic personal information to others who can protect it; and 5) protect NPI with the same level of protection that you would apply to your own confidential information.

Kenneth Klein (California Western School of Law) detailed the last of the privacy principles: 6) delete or de-identify NPI when it is no longer needed to process transactions necessary to fulfill the consumer's business with you or to fulfill legal obligations; 7) give consumers timely notice of any breach of their NPI and provide them with an actionable remedy for such breaches; and 8) your obligations under these principles are not waivable.

Matt Gendron asked the consumer representatives about deleting NPI when recent cases, such as Holocaust cases, where insurers hold on to data, have benefited consumers. Klein said these are principles rather than strict model law wording.

Robert Wake concurred that data retention is bad in some situations, but others where data trails can be good. He mentioned archiving data in secure locations where it cannot be used unless it is specifically summoned out of the storage. There is still some security risk, but it would prevent misuse.

Director Gillespie asked the consumer representatives if any parts of the chair draft did not adhere to the outlined principles. Dr. Ting noted that recently released Section 5 revisions to the chair draft embody these principles.

Frank Marnell noted that principle six on breaches conflicts with the *Insurance Data Security Model Law* (#668). Ellsworth stated that even though privacy and security are different, the way licensees implement control of data is a privacy concern.

5. Discussed Next Steps for Drafting Amendments to Model #672

Director Dwyer noted that the Working Group requested comments on Article III of the chair draft. Comments are due Nov. 25. The Working Group will hold an open call to discuss those comments in December.

The Working Group also released the revised Section 5 via email Nov. 11, and the language is available under Exposure Drafts on the Working Group's web page. This language was exposed as a result of the drafting group's Oct. 31 and Sept. 30 calls and the Working Group's Nov. 4 call. Comments are not being requested on Section 5 at this time. Comments will be requested after the next full exposure of the model.

The Working Group will continue to work through sections of the chair draft until it comes to a consensus on a draft for exposure.

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

SharePoint/NAIC Support Staff Hub/Committees/H Cmte/ 2024 Fall/Privacy/Minutes/Minutes-PrivacyWG111724-Final.docx

Draft: 11/26/24

Cybersecurity (H) Working Group
Denver, Colorado
November 18, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Denver, CO, Nov. 18, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair, and Eric Lowe (VA); Sian Ng-Ashcraft (AK); Chris Erwin (AR); Bud Leiner and Alena Caravetta (AZ); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Elizabeth Nunes and Matt Kilgallen (GA); Lance Hirano (HI); Mathew Cunningham(IA); C.J. Metcalf and KC Stralka (IL); Shane Mead (KS); Mary Kwei and Kory Boone (MD); Jeff Hayden and Jake Martin (MI); Jacqueline Olson and T.J. Patton (MN); Troy Smith (MT); Tracy Biehn (NC); Jon Godfread and Colton Schulz (ND); Christian Citarella (NH); Nick Stosic (NV); Gille Ann Rabbin (NY); Matt Walsh (OH); Michael Humphreys and David Buono (PA); John Haworth (WA); Andrea Davenport (WI); and Lela Ladd (WY). Also participating was Matthew Gendron (RI).

1. Adopted its Oct. 30 Minutes

The Working Group met Oct. 30. During this meeting, the Working Group took the following action: 1) adopted its Oct. 8 minutes, 2) heard an update on the progression of the Cybersecurity Event Response Plan (CERP) portal and the insurance data security model (IDSM) survey, and 3) heard a presentation on the NAIC's 2024 Cyber Insurance Report.

Haworth made a motion, seconded by Diederich, to adopt the Working Group's Oct. 30 minutes (Attachment Three-A). The motion passed unanimously.

2. Heard comments on the Confidential Cybersecurity Event Repository and Portal

Peterson described the project as a rare and exciting opportunity where both regulators and the industry are relatively aligned. Regulators intend for the portal to: 1) initially be focused on facilitating the transmission of event notices pursuant to the *Insurance Data Security Model Law* (MDL #668); 2) be focused on Model #668 reporting requirements, narrowing the information provided by the companies and reporting it to regulators via the portal; and 3) enable functionality to allow updates or amendments to the initial notice submitted to the department of insurance. There is an often-occurring problem where notification requirements grow, and it seems to be making compliance increasingly difficult.

Peterson reiterated the commitment to fully test and demonstrate the confidentiality and security of the portal. He explained that the project would be split into two motions. The first would require building a test portal to demonstrate general functionality, security, and access controls, initially built to meet obligations under Model #668. The second will seek to implement the portal into use for those states that have passed Model #668, and to plot future improvements to achieve regulatory convergence. Peterson suggested that a large tabletop exercise could be used to demonstrate how the concerns of stakeholders were addressed. He said the NAIC has the experience of developing the appropriate portal.

Kristin Abbott (American Property Casualty Insurance Association-APCIA) delivered public comments on behalf of its members, expressing support for the development of this portal and offering the organization as a resource as the project moves forward.

Lindsey Klarkowski (National Association of Mutual Insurance Companies-NAMIC) spoke on behalf of mutual insurance companies, agreeing that the process to report cybersecurity events and incidents needs to be streamlined. Klarkowski offered concern for the proposed portal because it could present a systemic risk if it is not intentionally narrow in breadth and function or structured with strong security and governance protocols. She suggested the portal would become a prime target for cybercriminals, as it would contain sensitive information about a large swath of the financial services sector and their breach and response measures. NAMIC suggests that rather than a centralized database or repository, the Working Group should consider a platform for the management of the issues where the licensees subject to Model #668 provide initial notification to departments and then a lead regulator coordinates communicating the substantive information. Klarkowski recommended that the sensitive information remains dispersed among companies and departments, avoiding the risk of a centralized and concentrated target opportunity.

Peterson opined that the information required under Model #668, Section 6B, is not particularly sensitive but rather represents information about a mitigated issue. He argued that more useful information is readily available on the dark web. He stated that currently, states accept notifications, and the amount of security offered can differ from state to state.

Peterson and Klarkowski discussed the concerns raised about the portal becoming a centralized source of insurance company information, and both agreed that further discussions with membership to get specifics would benefit the conversation.

Miguel Romero (NAIC) suggested that it would be helpful to hear from specific companies about how they have previously reported some of the information. He recalled that the language that is provided to departments is desensitized, including enough information so that the department understands what happened but not so much that it would include any proverbial keys to the kingdom.

Amann thanked NAMIC for its comments, reminded the group that the tabletop exercises would be the venue for anticipating and discussing some of the hypotheticals, and invited Working Group members to provide comments to the group.

Diederich pointed out the common vulnerabilities and exposures (CVE) identifiers and the associated website. He stated that since 1999, there has been a standardized reporting framework for identifying commonly experienced exploits that many entities might be subject to. Klarkowski said NAMIC's concern is about the creation of a new repository, bringing together a concentration of risk and fixed information related to the insurance industry. She encouraged stakeholder involvement to discuss what other pieces of Model #668 are the more sensitive pieces from the industry standpoint.

Boone explained that as a state with a portal where companies submit their documents, he has seen sensitive information in there. He understands NAMIC's concerns about hackers using the information to their advantage, because it often includes a company's security architecture and mitigation efforts.

Haworth described a scenario where NAMIC's primary concerns would be a situation where a hypothetical company, as an insurance carrier and underwriting company, uses file sharing software for remote employees. They discovered that it was hacked, so they mitigated and reported it, but they used two or three third party administrators who might still use the software, creating a risk exposure with downstream contractors and vendor relationships.

Gendron explained that in Rhode Island, the department has 30 employees, and their data security is handled by the state agency. He said the NAIC has considerably more data security people than Rhode Island and would be better equipped to hold confidential information. When Own Risk and Solvency Assessment (ORSA) or Market Conduct Annual Statement (MCAS) filings are received, they go to the NAIC and not Rhode Island. For many years, the NAIC has been an incredibly safe and secure receptable for very confidential information from insurance companies. Gendron suggested the portal would also be a measure to save costs for insurers having to pay legal fees for providing multiple notifications for single events.

Buono thanked NAMIC for its comments and said an additional concern would be ensuring internal employees are not given inadvertent access. He suggested restricting the information received in the portal to only the appropriate users.

Romero suggested that the membership consider having the NAIC work with the Working Group Vice Chair to develop and document the project in a memo to be presented as materials in a future Working Group meeting.

Diederich made a motion, seconded by Chou, to authorize the Working Group to work with the NAIC to explore the creation of the cyber security event notice portal. The motion passed, Maryland and New York abstained.

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

Rocco Grillo and Scott Harrison (Alvarez & Marsal) gave an informative presentation titled "Surviving the Firestorm of a Cyber Incident." The presentation highlighted their learned best practices for surviving the firestorm of a cyber incident, the many ways a cyber threat might victimize a company, and some trends observed in recent years. As a service provider, Alvarez & Marsal prioritizes helping its customers understand that they cannot necessarily stop attacks, but they can be better prepared to respond to and recover from cybersecurity incidents. The presentation also provided a reminder that an incident response plan requires ongoing enhancements in response to new technologies, increasing sophistication in attacks, and the evolving regulatory landscape.

The threat landscape continues to evolve, and Grillo explained that as companies continue to innovate to get a leg up on their competition, it creates exposure. Ransomware or cyber extortion has been around for years however, in the last five or so years there has been a significant increase in instances of ransomware attacks. Ransomware as a service and double extortion or even triple extortion attacks continue to victimize companies. He explained that more victims are having their data encrypted and then exfiltrated. Cyber criminals with the data exported will often accept an initial ransom payment to "unlock" the company data, but then demand a second ransom to not release the victim's data on the dark web.

Grillo explained a growing trend has been observed with threat actors going after mid-size and smaller companies that have little to no backups, resilience, or the ability to recover. Referring to it as "mid-game hunting," Grillo explained that in these instances even if it's a heavily regulated entity like a small bank, they may not have the ability to recover from a single cyber incident and are forced to close. He suggested that even companies that have transitioned to cloud-based services could face significant financial loss from a connection being inadvertently compromised by a third-party contractor.

Grillo asked those in attendance to consider whether they had ever used the same password for their personal account that they do for a work account, explaining that if a threat actor had your compromised password, a simple internet search could allow them to identify where you work and use the password as part of a brute force

attack. He explained that compromised credentials are used in supply chain attacks, comparing it analogously to a thief targeting a high rise on Park Avenue in New York. Most thieves would go straight to the penthouse for the crown jewels, but a cyber threat actor mindset would have them go to the superintendent's office, get the keys to every apartment, and drain the whole building before leaving. Grillo explained that the Federal Bureau of Investigations (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) work in partnership with victims of cyber crimes to help them investigate and recover.

Speaking about the tabletop exercises facilitated by the Financial Services- Information Sharing and Analysis Center (FS-ISAC), Grillo explained that he was part of the inaugural team in 2010. Companies with an incident response plan should practice and ensure they have relevant playbooks to support their plan for various types of incidents. They should review and update those plans annually and ensure the content aligns with changes in insurance coverage or technology enhancements as well as business processes. Grillo encouraged driving resilience and ensuring external stakeholders, communications teams, and law enforcement partners are included in the planning and testing of the incident response process.

Providing closing thoughts on addressing risk, Grillo suggested increasing visibility into the infrastructure to remain aware of what baseline healthy performance is to increase response to anomalies. He said companies should reduce the attack surface level risks, prevent known risks, and try to uncover unknown risks, by exploring their most critical assets and simulating how they could be exposed to new technologies or different ways of doing business. They should also quantify the analysis to ensure the right controls are in place and they have enough people and processes to rely on. If a company does not, does it have the right coverage or enough of it in place? Grillo said cyber insurance is important, but it is not the end all, as it only alleviates the financial impact of a risk.

4. Heard an Update on Lines of Efforts Being Pursued by Working Group Members.

Mead discussed the quick work done by the drafting group under the Information Technology (IT) Examination (E) Working Group. Tasked with a two-part process, the drafting group completed part one, which was to perform a gap analysis of Exhibit C to National Institute of Standards and Technology (NIST) procedures and the Cyber Security Framework 2.0 and provide suggestions. The second step which will extend into 2025 will separate procedures needed to establish the liability of IT general controls from those needed to examine cybersecurity. The drafting group will take care to ensure that findings concerning IT general controls can be made before the end of phase two of the financial examination, while it is possible that findings on cybersecurity matters may take place later in the exam process.

Mead stated he believed some of the current procedures in Exhibit C could be eliminated during the process, suggesting they may be found redundant or no longer relevant. He said it is important that the resulting IT general controls and cybersecurity reviews remain appropriately sized for examination purposes.

Schulz provided a short update on the data calls and definitions work to help regulators understand the various data types and definitions, where they can be found and accessed, and what information is not available with the current data. He said the work to inventory and index the data elements that the industry reports to the NAIC should substantially complete by the end of 2025.

Chou said the American Academy of Actuaries (Academy) intends to revisit their cyber toolkit and is pursuing a partnership with CyberCube Analytics, which is focused on data management topics.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_fall/WG-Cybersecurity/Minutes-CyberWG111824.docx

Draft: 11/16/24

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

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

1. Adopted Its Oct. 8 Minutes

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

Schulz made a motion, seconded by Buono, to adopt the Working Group's Oct. 8 minutes (Attachment Three-A1). The motion passed unanimously.

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

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

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

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

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

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

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

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

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

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

3. Heard a Presentation on the 2024 Cyber Insurance Report

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

Henry gave a market overview, stating that global premium reached $16.66 billion for cyber coverage in 2023, and the U.S. cyber insurance market remains the largest with a 59% market share. Henry stated that the cyber threat landscape continues to break records as it becomes more volatile and complex, and global cyber insurance premiums are projected to exceed $50 billion by 2030. The increasing number of cyber incidents is driving demand for appropriate coverage to mitigate financial losses. He further explained that small- and medium-sized enterprises (SMEs), a particularly vulnerable business sector, are expressing interest in cyber insurance, as companies in all revenue bands are targeted. An 11% increase in policies in force counts reflects a growing demand

for cyber insurance coverage. Henry stressed the importance of maintaining good cyber hygiene practices and not allowing growth in the comfort and stability of the cyber insurance market to be viewed as an opportunity to become complacent. Referring to 2023 claims data, Henry reported ransomware and business email compromise claims were trending up in frequency and severity. Companies earning more than $100 million in revenue saw a 20% increase in the number of claims and a 72% increase in claims severity compared to the second half of 2022.

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

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

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

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

Chou asked if Henry could provide additional input on how state insurance regulators might be able to provide the necessary education or incentives to help increase the awareness of and take up rate for cyber insurance. Amann suggested that while it might be a complicated answer, state insurance regulators should step up the focus

and discussion of cyber hygiene and cyber event prevention. Amann said there is still a need for good cyber practices, oversight, and continued education and that buying coverage is just the first step. She suggested collecting and analyzing cyber data is the best way to understand the marketplace, allowing the state insurance regulators to understand the commonly used exclusion language or policy limitations.

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

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

Draft: 10/28/24

Cybersecurity (H) Working Group
Virtual Meeting
October 8, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met Oct. 8, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Julia Jette (AK); Leo Liu (AR); Bud Leiner (AZ); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Matt Kilgallen (GA); Daniel Mathis (IA); C.J. Metcalf (IL); Shane Mead (KS); Mary Kwei (MD); Jeff Hayden (MI); Troy Smith (MT): Tracy Biehn (NC); Colton Schulz (ND); Christian Citarella (NH); Scott Kipper (NV); Gille Ann Rabbin (NY); Don Layson (OH); David Buono (PA); Andrea Davenport (WI); and Lela Ladd (WY).

1. Adopted Its Sept. 4 Minutes

The Working Group met Sept. 4 and took the following action: 1) heard a presentation from AM Best on the cyber insurance market, which assigned a stable outlook on the global cyber insurance market.

Schulz made a motion, seconded by Buono, to adopt the Working Group's Sept. 4 minutes (Attachment Three-A1a). The motion passed unanimously.

2. Heard a Presentation from the FBI Internet Crime Complaint Center (IC3)

Rachel Yurkovich (Federal Bureau of Investigation—FBI) introduced the IC3 program and discussed its inclusion in the Cyber Division and the Criminal Investigation Division of the FBI and how those roles intersect. She explained how the FBI's mission priorities have increasingly focused on cyber threats, including ransomware, intrusions, and tracking cyber adversaries. IC3 provides a central reporting mechanism for the public and the FBI regarding cyber intrusions and scams. For law enforcement, it provides remote access to a database of complaints received since 2000. Its website (ic3.gov) offers public service announcements, consumer alerts, and annual reports. Yurkovich described the IC3 partnerships with private sector entities and various government agencies at all levels.

Yurkovich explained that nearly every complaint received by IC3 is reviewed, confirming crime types, loss reporting, and adjusting where necessary in the case of fraud scams. The organization receives an average of 2,900 complaints a day. She described the increasing trend of extortion emails, which include pictures scraped from Google Maps, suggesting that the scammer has proof of the victim in a compromising act and/or visiting bad websites, and the scammer demands payment in Bitcoin. In addition to complaint processing, the IC3 provides case support, complaint aggregation, and reporting, as well as call centers supporting fraud claims. 2024 has already exceeded the $12.5 billion dollars of loss reported in the year 2023. Yurkovich described how the number of complaints received seemingly averaged while the losses significantly increased over the last five years. She stated that losses reported often do not include the cost of recovery, such as a business or an individual having to start over.

Introducing the term "pig butchering," Yurkovich explained it is a type of crypto-based confidence investment fraud where a victim meets someone online and builds a relationship with them. She clarified that the relationship does not necessarily have to be romantic; it could be a professional relationship stemming from a LinkedIn connection, for example. Eventually, the scam artist, turned friend, convinces the victim to invest in crypto. This type of fraud usually develops over a period of a month. The victims start by investing a little bit at a time, and the fraudster portrays positive earnings and might even allow a small payout in order to build trust. Yurkovich said at some point in time, the victim attempts to collect, and that is when the veil is lifted. They realize everything is

gone. Reporting victims come from all age ranges. However, 30- to 49-year-olds have been the most impacted, and devastatingly, some of these victims lose their entire savings and retirements to these scams.

Discussing major cyber threats observed by the IC3, Yurkovich stated they received 1,193 complaints from organizations belonging to a critical infrastructure sector that were affected by a ransomware attack in 2023. Of the 16 critical infrastructure sectors, IC3 reporting indicated 14 had at least one member that fell victim to ransomware last year. The most targeted sectors were 1) healthcare and public health, 2) critical manufacturing, and 3) government facilities. IC3 typically receives ransomware complaints from victims after systems have been infected but prior to a ransom being paid. The FBI does not encourage ransom payments but realizes businesses have an obligation to get their systems back up and running as soon as possible.

Tom Wetzel (Wetzel and Associates) asked if there was any uptick in crime observed in the wake of any natural catastrophes. Yurkovich explained there is always an uptick, especially charity fraud, with people posing as legit charities to elicit monetary donations.

Smith asked for an explanation of "advance fee and overpayment" as labeled on a graphic of reported crime categories. Yurkovich said some people are applying for government grants or loans online, and they are given upfront fees and taxes to be paid ahead of time to get the funds. It is a common weak point in the industry, and fraudsters know it, so they take advantage of it, accepting the upfront payments and disappearing. Conversely, overpayment and non-delivery fraud seek to send "extra" money in hopes of collecting. Yurkovich gave the example of someone selling an item on eBay for $500. The fraudster purchases the item but sends a check for $2,000 with instructions for the seller to give the $1,500 of overpayment funds to the person picking up said item. Once complete, the check bounces, and the seller turned victim is out $2,000, their item, and whatever fees are demanded by their bank.

Diederich asked whether ransomware is primarily targeting financial gain or if the exfiltration of information is the underlying objective of the intrusion. Yurkovich expounded on the topic of ransomware trends, specifically explaining the double extortion tactic where the ransomware groups lock down or encrypt files while simultaneously exporting and storing them. They then demand a ransom, and if the company pays, they unlock the files. Having stored the data, the group comes back to the victim company a few months later, demanding a ransom or the data will be released on the web. Yurkovich observed a growing trend of multiple groups, especially more prominent groups, targeting the same victim with different types of ransomware variants.

Yurkovich explained how business email compromise is a type of scam carried out by a subject compromising legitimate business or personal email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds. Either through monitoring active email traffic or reviewing past requests, they identify who is allowed to approve payments and who is allowed to request payments be sent somewhere different. Yurkovich suggested only after extensive research or the use of tools, the subjects formulate emails impersonating the appropriate individuals to request payment reroutes. 2024 has seen an increase in business email compromise targeting the real estate sector, with cyber criminals portraying the real estate agency to reroute down payment wires.

Debra Decker (Stimson Center) asked what the benefits of reporting to the FBI are for businesses and the public, across all crimes and ransomware cases. Reiterating that reporting to IC3 is voluntary, Yurkovich explained that increased awareness of reporting could help the FBI understand and track the trends of reported crimes. Observing an aggregated condition, such as a specific area reporting real estate-related activity, allows the FBI to redirect resources and allocate case agents effectively.

In 2018, the IC3 started the recovery asset team, which is specifically for business email compromise scams. However, Yurkovich explained they have expanded to include any crime type reported as a complaint to the IC3. She added that if the complaint is submitted within 10 days of a wire or an ACH transfer and meets certain thresholds, the recovery team can assist in recalling the funds for the victim. In 2023, they reported a 71% success rate, recovering $538 million for more than 3,000 incidents.

Yurkovich explained the IC3 partners with U.S. government agencies, foreign law enforcement, as well as private sector organizations, such as the National Cyber-Forensics and Training Alliance (NCFTA). She also provided reporting resources:

- Internet Crime Complaint Center
  - www.ic3.gov
- National Threat Operations Center
  - www.tips.fbi.gov
  - 1-800-CALL-FBI (225-5324)
- National Elder Fraud Hotline
  - 833-372-8311

Chou asked how the American Academy of Actuaries (Academy) could get access to the IC3 data-sharing protocols. Yurkovich explained that the remote query-sharing program is temporarily paused for organizations outside of sworn law enforcement. IC3 is conducting an internal review and overhaul of the remote query access to ensure maximal security for victim information.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Fall/WG-Cybersecurity/2024 1008Interim-Meeting/Minutes-CyberWG100824.docx

Draft: 9/11/24

Cybersecurity (H) Working Group
Virtual Meeting
September 4, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met September 4, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Chris Erwin (AR); Bud Leiner (AZ); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Matt Kilgallen (GA); Lance Hirano (HI); Daniel Mathis (IA); C.J. Metcalf (IL); Shane Mead (KS); Mary Kwei (MD); Jake Martin (MI); T.J. Patton (MN); Tracy Biehn (NC); Colton Schulz (ND); Martin Swanson (NE); Christian Citarella (NH); Scott Kipper (NV); Gille Ann Rabbin (NY); Don Layson (OH); David Buono (PA); Bryon Welch (WA); Andrea Davenport (WI); and Lela Ladd (WY).

1. Adopted its Summer National Meeting and Aug. 1 Minutes

The Working Group met Aug. 1 and took the following action: 1) heard an update from Shana Oppenheim (NAIC) regarding her observations of federal cybersecurity and cyber insurance activities.

Schulz made a motion, seconded by Buono, to adopt the Working Group's Aug. 14 (*see NAIC Proceedings, Summer 2024 – Innovation, Cybersecurity, and Technology (H) Committee, Attachment Three*) and Aug. 1 minutes (Attachment Three-A1a1). The motion passed unanimously.

2. Heard a Presentation from AM Best on the Cyber Insurance Market

Michael Lagomarsino and Tom Mount (AM Best) gave an informational presentation to the Working Group on the U.S. cyber market and AM Best's cyber initiatives. Lagomarsino said AM Best assigned a stable outlook on the global cyber insurance market. Some of the positive factors supporting that outlook include continued demand, increasing take-up rates for cyber insurance coverage, and continual improvements in cyber hygiene. Greater take-up rates, primarily in small and medium enterprises (SMEs), will drive growth over the next five to ten years. He said improvements in underwriting practices and risk selection practices of insurers have driven investments in cyber security. Additionally, cyber insurance turned to incorporating exclusionary language around critical infrastructure and war as an action to reduce exposure to aggregate losses. Lagomarsino said the market has been supported by reinsurance, with roughly 50% of premium ceded to reinsurance. Several cyber catastrophe bonds have been issued over the last 12 months on the public market. This is a positive sign that investors are getting more comfortable with how cyber is being underwritten.

Lagomarsino introduced several countervailing factors the global cyber insurance marketplace faces, including increased competitive pressure and additional capacity entering the market. AM Best is watching how the market responds to recent high-profile cyberattacks; however, to date, insured losses from these recent incidents appear manageable. The attacks serve as a reminder of uncertainty over the aggregation of risk, the growing sophistication of attacks using artificial intelligence (AI), and the dynamic nature of the cyber risk environment. Lagomarsino explained that any reduction in reinsurance capacity would reflect a reduction in cyber risk appetite on the primary side, which could result in significant market dislocation.

Discussing trends observed in the U.S. cyber insurance market, Lagomarsino explained that there was a deterioration in the direct loss and defense and cost containment (DCC) loss ratio, driven by a significant increase in the frequency of ransomware attacks at the onset of the COVID-19 pandemic. Companies aggressively invested in technology to enable remote work environments, leading to significant losses. Insurance companies reacted

with significant rate increases while tightening terms and conditions, specifically increasing deductibles and putting sub-limits within the policies. The aggressive actions, in conjunction with improved cybersecurity hygiene, resulted in significant improvement in underwriting results. Lagomarsino observed that premiums experienced significant growth in 2022 and flattened in 2023, but profitability remains strong and is expected to remain in place for the foreseeable future. Citing a report by Howden, he added that global cyber insurance premiums are three times higher than pre-COVID levels; however, they have flattened and are even turning negative more recently. Summarizing post-COVID trends in cyber claims, Lagomarsino stated that year-over-year (YOY) growth has been driven by first-party claims, which tend to be shorter-tailed in nature and enable carriers to respond quicker. He said the increased frequency of ransomware attacks since the COVID-19 pandemic continued to hit record levels in 2023. Due to improved cybersecurity hygiene, though, the percentage of companies impacted by a ransomware attack that are paying the ransom has significantly come down over time, which should reduce claim severity.

Mount delivered a detailed overview of AM Best's credit rating methodology and the building block approach. He explained rating considerations for affirmative cyber and highlighted some areas of a balance sheet that cyber would affect. He described why incorporating catastrophe risk and stress testing is necessary and could effectively manage exposure to catastrophe events, which is essential to protecting and preserving balance sheet strength. Mount gave examples of how catastrophe modeling could look at historical losses and conduct deterministic scenarios for estimating loss. He described a cyber catastrophe as a shock loss, which is usually a large and sudden loss with a shorter tail. Additionally, he said some challenges for cyber stress testing are in how various models differ. While some have similar assumptions, others might better capture a certain type of exposure or risk.

Mount explained the AM Best team is developing a cyber questionnaire to help understand the growth in affirmative cyber writing and to quantify and understand the impact of cyber risk management. The general questions he described sought to answer the nature of the portfolio, cyber risk appetite, and underwriting strategy to better understand the use of third parties.

Concluding their presentation, Lagomarsino explained that many companies manage cyber risks through underwriting and risk transfer as well as through policy wording, like the war exclusions. He described companies as being mindful of the rate component versus the terms and conditions, as they are focusing on managing their aggregates in the underwriting process.

In recognition of the elapsed time, Amann suggested that the meeting's question-and-answer (Q&A) portion be skipped to allow the vice chair to discuss a requested update. She expressed appreciation for the guest speakers and welcomed Peterson to address the Working Group.

3. Received a Chief Financial Regulator Forum Referral

Amann informed the Working Group to expect an email following the meeting to discuss the referral received by the Chief Financial Regulator Forum.

4. Discussed Other Matters

Peterson gave an update on the activities following the adoption of the Cybersecurity Event Response Plan (CERP), which is developing a confidential repository for cybersecurity event notification. The CERP is intended to be guidance for departments of insurance (DOIs) when they must respond to a cybersecurity event. Peterson explained that the building of a notification portal requires that the state insurance regulators achieve agreement on two primary concerns: 1) whether it will meet the needs of the state that has passed its own version of the *Insurance Data Security Model Law* (#668); and 2) whether it will fill the confidentiality and security commitments

made to the industry. Peterson discussed the Model #668 survey under development and offered the idea of a proof of concept as a step to provide the necessary understanding. He suggested the Working Group ask NAIC staff to build a narrowly scoped notification portal for initial assessment. Peterson said it would be accessible initially to the states with their own version of Model #668, and the initial fit would be those questions in Section 6B. Peterson said the proof of concept and the survey to the states should give state insurance regulators an understanding of the confidentiality and security measures expected in order to pass a formal motion to begin the testing and future implementation of the portal.

Amann suggested a Working Group call in the future to discuss the Model #668 survey and notification portal project.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Fall/WG-Cybersecurity/2024 0904 Interim-Meeting/Minutes-CyberWG090424.docx

Draft: 8/6/24

Cybersecurity (H) Working Group
Virtual Meeting
August 1, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met August 1, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Julia Jette (AK); Bud Leiner (AZ); Mel Anderson (AR); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Matt Kilgallen (GA); C.J. Metcalf (IL); Daniel Mathis (IA); Shane Mead (KS); Mary Kwei (MD); Jake Martin (MI); T.J. Patton (MN); Tracy Biehn (NC); Colton Schulz (ND); Christian Citarella (NH); Scott Kipper (NV); Gille Ann Rabbin (NY); Don Layson (OH); Jodi Frantz (PA); Bryon Welch (WA); and Andrea Davenport (WI).

1. Adopted its May 29 Minutes

The Working Group met May 29 and took the following action: 1) heard a presentation from the Coalition on the "Effectiveness of Security Controls: A Meta Analysis."

Schulz made a motion, seconded by Chou, to adopt the Working Group's May 29 minutes (Attachment Three-A1a2). The motion passed unanimously.

2. Heard an Update on Federal Activities Related to Cybersecurity and Cyber Insurance

Shana Oppenheim (NAIC) provided an overview of her federal update, which included: 1) the Cybersecurity and Infrastructure Security Agency's (CISA) Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) Cyber Event Notice Rulemaking; 2) the effect of *Loper Bright Enterprises v. Raimondo* and the overturning of *Chevron* deference on cyber rulemaking policy; and 3) a general overview of federal activity around cyber insurance and cybersecurity.

First, CISA published the notice of proposed rulemaking (NPRM) for CIRCIA in March. Oppenheim said that insurers with $2 million to $47million in revenue and a 500–1,500 employee count will be exempted from this reporting. Insurance companies can act as third-party representatives for covered entities. This means they can submit cyber incident reports on behalf of their clients, provided they have explicit authorization. All other insurers will have to report to CISA within 72 hours of forming a reasonable belief that a covered cyber incident has occurred and 24 hours after paying a ransom. Covered cyber incidents fall into four categories: 1) substantial loss of systems integrity/confidentiality; 2) serious disruption of operations; 3) serious disruption of business; and 4) unauthorized access to non-public information. The reported data is concerned with incident management. CIRCIA requires covered entities to ensure preservation of relevant data and records associated with the reported incidents, and supplemental reports are required for new and different information becoming available.

Oppenheim said that the NAIC provided detailed comments on CISA's proposed rulemaking for CIRCIA. The comments submitted addressed the NAIC's support for clear guidelines, coordination with state insurance regulators, data protection and confidentiality, impact on small and medium-sized entities, and public-private collaboration. These comments reflect the NAIC's commitment to ensuring the CIRCIA rulemaking process results in practical, effective, and fair regulations for the insurance industry.

Second, Oppenheim described the key context of the Supreme Court's decision in *Loper Bright Enterprises v. Raimondo* and its significant implications for federal cyber regulations, particularly in the context of CIRCIA. She said the ruling eliminates the *Chevron* deference, which previously allowed courts to defer to federal agencies' reasonable interpretations of ambiguous statutes. This change means courts will now independently interpret statutes, potentially leading to more legal challenges against agency rulemaking. CISA's proposed rules under CIRCIA, which require critical infrastructure entities to report cyber incidents, may face increased scrutiny and legal challenges. Oppenheim said that critics, including those in the U.S. Senate, have already raised concerns. The Biden administration is considering changes for the National Cybersecurity Strategy in response to the *Chevron* impact. The decision complicates efforts to enforce security rules on critical infrastructure through executive orders, which relied on broad statutory interpretations. Despite these challenges, the administration plans to proceed with new cybersecurity regulations for the health care sector, even amid opposition from U.S. governors. Oppenheim opined that overall, the *Loper Bright* decision is expected to lead to more rigorous judicial review of federal cyber regulations, potentially slowing down the rulemaking process and necessitating closer collaboration with Congress.

Third, Oppenheim said the discussions around a federal backstop to catastrophic cyber insurance have been quite active in 2024. Across various federal agencies, Congress, and other stakeholders, these efforts are part of a broader initiative to support the existing cyber insurance market and address the increasing risks posed by cyberattacks on critical infrastructure. The Federal Insurance Office (FIO) and CISA have been working together to assess the need for a federal insurance response to catastrophic cyber incidents following a recommendation by a 2022 Government Accountability Office (GAO) report. FIO held a roundtable on this issue in Spring 2024, following the Fall 2023 conference it co-sponsored with NYU Stern's Volatility and Risk Institute (VRI), which brought together industry experts, policymakers, and stakeholders to discuss catastrophic cyber risks and potential federal responses. FIO also partnered with the National Science Foundation (NSF) to establish an industry university cooperative research center to focus on cyber and terrorism insurance. She said the center is trying to provide research that would improve the modeling and underwriting of both terrorism and cyber risks.

Oppenheim said Congress is continuing the discussion of a federal backstop with a hearing to discuss bipartisan support for harmonizing cyber insurance as the market evolves. However, there has not been inclusion of the topic in any legislative language.

Peterson asked if the supreme court opinion will have an impact on a federal organization's ability to take action. Oppenheim said that it would depend on what statute they are attempting to proceed under; CIRCIA could be vague enough that it would need to be amended to give a more specific set of instructions.

Schulz asked about Oppenheim's awareness of discussions to wrap cybersecurity into the Terrorism Risk Insurance Act (TRIA). Oppenheim stated she was not aware of any discussion because it might require amending TRIA. She said the meetings she has attended were more on how to model a cyber backstop and modeling it after TRIA or after the National Flood Insurance Program (NFIP).

Chou offered a reminder of the difference in modeling cyber and terrorism.

Lauren Pachman (National Association of Professional Insurance Agents) offered a comment on the last reauthorization of TRIA in which Congress considered adding cyber terrorism but opted against it. She suggested anticipating the Treasury would have challenges of doing this in the absence of *Chevron*.

Fourth, Oppenheim discussed the federal activity in cybersecurity, starting with the U.S. Securities and Exchange Commission's (SEC's) Cyber Incident Disclosure Rule, implemented last year, which necessitates enhanced reporting for transparency with investors. While CISA is driving for improved federal and public collaboration with

a harmonization on reporting rules, Oppenheim added that the SEC's division of corporation finance issued new guidance requiring companies to assess the materiality of ransomware incidents promptly and disclose them on Form 8-K if deemed material, even if the incident is resolved or a ransom is paid before the reporting deadline. She explained how CISA is trying to get more cybersecurity firms to aid in the event of a severe cybersecurity attack. She said that the CISA director mentioned this could include invoking emergency authorities like the Defense Production Act (DPA) and the National Emergencies Act.

Peterson asked about the federal attitude in response to the recent global information technology (IT) outage caused by CrowdStrike. Oppenheim said while no legislative drafting has surfaced, that could change following the company leadership's hearing at Congress.

Amann discussed the challenges of policy definitions not keeping up with the changing landscape of cyber. She thanked Oppenheim for keeping the Working Group informed on what the federal organizations are saying.

3. Heard a Preview of its Summer National Meeting Plan

Amann told the Working Group about the panel discussion at the Summer National Meeting, during which industry speakers will give their perspectives on the cyber insurance market. This panel is a result of the Working Group's plan to learn from industry experts by inviting them to make presentations to members of the Working Group focusing on actual business practices and less on theory.

4. Discussed Other Matters

Amann reminded the Working Group of the Catastrophe Insurance (C) Working Group's Catastrophe Modeling Primer and asked for participant input. Bubba Aguirre, an investigator in Minnesota, offered his experience investigating cybersecurity events and sharing fraud awareness information with residents. He asked whether other states are investigating cybersecurity incidents reported to them. Peterson offered scheduling a meeting to speak about this topic in a session to provide an update of what other states are doing to address this issue.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Summer/WG-Cybersecurity/Minutes-CyberWG080124.docx

Draft: 7/10/24

Cybersecurity (H) Working Group
Virtual Meeting
May 29, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met May 29, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Bud Leiner (AZ); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Tia Taylor (GA); Daniel Mathis (IA); C.J. Metcalf (IL); Shane Mead (KS); Mary Kwei (MD); Jake Martin (MI); T.J. Patton (MN); Martin Swanson (NE); Tracy Biehn (NC); Colton Schulz (ND); Christian Citarella (NH); Gille Ann Rabbin (NY); Matt Walsh (OH); David Buono and Sebastian Conforto (PA); Rebecca Rebholz (WI); and Lela Ladd (WY).

1. Heard a Presentation from Coalition on the "Effectiveness of Security Controls: A Meta Analysis"

Amann opened the meeting by discussing the planned 2024 presentations on cybersecurity and staying informed of related market trends. She thanked Sezaneh Seymour (Coalition) and Daniel Woods (Coalition) for taking the time to present, noting the high caliber of their important and relevant work.

Seymour expressed how the cyber insurance landscape is changing and how cyber insurers have become a more central part of the security conversation. She said Coalition approaches cybersecurity risk with an active insurance model. Its data suggests policyholders experienced 64% fewer claims than the market average, consistent over the previous few years. Seymour said the evolution of cyber insurance has grown to be more than just a mechanism to transfer financial risk—cyber insurance has become a market-based tool to drive security improvements across businesses and infrastructure. She said Coalition has a team of security experts available to provide technical assistance throughout the policy's life cycle.

Woods began presenting the research by highlighting the key understanding that while cybersecurity is a mainstream national security issue, cyber risk science is difficult. He stated that Coalition's systematic academic literature review reveals an immature body of research. Woods said the research he conducted shows that cyber insurers are beginning to produce evidence not available in scientific literature. They looked at academic and industry research to identify common threads, one of which was the importance of patch management. One study by Gallagher Re found that the speed at which patches are applied is the most important technical predictor of the likelihood of suffering a claim. Woods said the study noted that revenue and industry are still the most important, but when it comes to technological controls, patch cadence seems to be the most important.

The second finding identified multi-factor authentication (MFA) as a highly effective control for protecting individual accounts. Woods said that one outside study identified a 99% reduction in compromise of individual accounts, while another study conducted during the same period found that implementing MFA was associated with the lowest reduction in claims likelihood compared to 10 other controls. The Marsh study sourced questionnaires filled out by clients looking to buy cyber insurance; however, self-reported information continues to be unreliable because a simple "yes" or "no" response is not enough information. Woods highlighted the Change Healthcare incident, wherein the organization had MFA in some places but, for whatever reason, did not apply it to its corporate virtual private network (VPN). Coalition is trying to innovate by taking steps to move away from a checkbox questionnaire insurance application form.

The third important control is attack surface management, which is essentially how organizations configure web infrastructure with which attackers can interact. A key insight is that the revolution of the internet was connectivity, as it created many economic opportunities through connections. When viewed from a security

perspective, it creates problems because, in theory, a threat actor could interact with them and potentially compromise security. Attackers can probe any part of the organization's attack surface, and there is no single attack surface to close down. Coalition found that businesses with internet-exposed remote desktop protocols (RDPs) are two-point-five times more likely to file a claim. Ransomware gangs exploit this protocol because it essentially is designed for support, allowing someone from the outside to have total control over the device.

The final control or area of concern is what is referred to as perimeter products or boundary devices. Coalition found one corporate VPN associated with a five-times increase in claims frequency. If a cyber actor can find a vulnerability in one of these types of devices, they could compromise many different organizations with the same type of device on the network.

Seymour provided reflections for state insurance regulators; the research has provided data-driven epiphanies of the obvious, which are to reduce the attack surface, patch cadence, and deploy MFA. Each of these is likely to move the needle with respect to an organization's security. Seymour emphasized how this type of research would not have been possible even several years ago because cyber insurers have only recently started to make this data available. She further explained that Coalition recognizes a bespoke approach to cyber insurance is required to accurately measure and effectively mitigate cyber risk. Seymour concluded the presentation with several observations and recommendations for consideration. First, she said that Coalition encourages the option to rate without filing, and where that is not an option, approval timelines need to accelerate dramatically. Second, it encourages state insurance regulators to keep the mutually reinforcing nature of cyber insurance and security services in mind, allowing insurers to offer discounts when policyholders implement risk reduction measures. Third, in the context of ongoing work on data privacy, it encourages being mindful that the goals of transparency and data minimization do not inadvertently undermine ongoing threat research and information sharing in the cybersecurity space.

Chou opened the question-and-answer (Q&A) period by providing a high-level review of the relationship between the regulatory body and the role the filing process plays in securing and addressing solvency concerns, specifically encouraging the industry to work together to discuss when any state's response is too slow, or they may identify opportunities for accelerating the review process.

Amann inquired about insurers putting requirements on client companies to implement risk reduction measures and whether Coalition has received pushback on the matter. Seymour explained how they evaluate a potential new policyholder through a risk assessment, resulting in a risk profile category. Coalition does not require policyholders to have perfect security, but it reserves the right to make coverage contingent on the policyholder correcting any critical vulnerabilities identified. Woods provided additional insights into the resources of its policyholders, which are mostly small businesses, explaining that they do not have the ability to manage 3,000–4,000 vulnerabilities each month. The Coalition team works to identify the vulnerabilities most likely to be exploited by threat actors and sends those notifications to their clients, guiding insurance toward the most effective interventions. Amann opined that state insurance regulators should develop something along the lines of the National Institute of Standards and Technology (NIST) framework for some regulatory expectations of what insurers are required to do.

Unal Tatar (University at Albany) asked a question about what impact Coalition sees government initiatives in software vendor liability having or will have on reducing the risk level for buyers and an impact on cyber insurance. Woods responded with a personal view from an academic perspective. He explained that when an organization adopts Cisco, it has a particular product with a 500% increase in the probability of having a cyber insurance claim. This is where software liability could be relevant because the policyholder probably had no idea when they bought the product five years prior. The assignment of liability by state insurance regulators could be interesting because the vendors essentially need to be held accountable for building insecure software. This accountability is what

motivated the discussions at the federal level. Woods suggested there is a role for insurers to segregate against those vendors given the kind of increased information available. Seymour reflected on how today's burden for security, in software and misconfigurations, is disproportionately placed on the end users of those technologies. The system in which the insurance world is navigating is often the consumers who are the least placed to secure technology. In order to shift the burden, it is important for the organization to effectively manage controls like limiting attack surface and patching cadence.

Chou asked Woods to provide more information regarding the patch management example in the presentation material, wherein the vulnerability and patch were published Oct. 10, but a week after, threat actors were detected to be exploiting the vulnerability. Chou asked whether some users have not updated their systems and how it can be prevented if that is the case. Woods explained how many organizations are not fully resourced and ready, which could have avoided this incident. If a system administrator is applying to a crucial VPN enabling remote employees to continue working, if there is an error in doing so, it could lead to all of those employees not being able to produce work for a day. System administrators want to test and ensure the patch is reliable, which is something Coalition is attempting to address through prioritization.

Peter Kochenburger (Consumer Representative) asked for an example where legislation or regulation is designed to increase transparency and reduce the amount of data needed to the absolute minimum. Woods described how the legal interpretation of attorney-client privilege and work product doctrine applies to digital forensics investigations. Specifically, how some investigations are found to not be protected by privilege because they are not conducted for the purpose of advising lawyers. He noted that some digital forensics firms stop writing down incident investigations, which means those findings cannot be used to advocate for improvements after the incident to share threat intelligence.

Schulz asked about a list or a database of minimum standards that could be used by information technology (IT) examiners to see that companies are meeting the minimum standards. Seymour and Woods provided information on the machine learning (ML) system at Coalition that scores vulnerabilities from the national vulnerability database. Organizations should look to patch the vulnerabilities with a higher score, prioritizing the ones most likely to be exploited.

Peterson explained how cyber insurance covers unusual risk, as it is much more dynamic, and asked how the presenters generally predict the industry evolving. He further asked if Coalition thought that in the future, the people who write insurance policies will also be the same people doing gap analysis. The speakers jointly described how insurers are likely going to need to either partner with security service providers or become one themselves. Woods remarked that carriers cannot just sell a PDF for peril, adding that the sale must be alongside security.

Diederich asked the speakers to discuss the challenges posed by legacy systems or the bespoke in-house applications, some of which may be old and not currently patched. Woods described how some of the critical sectors, like health care, might have legacy systems running on Windows XP and how the recommendation would be for them to take those systems offline, partly because security is not a product so much as it is an ongoing process and requires active care.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Summer/WG-Cybersecurity/Minutes-CyberWG052924.docx

Draft: 12/3/2024

Adopted by Executive (EX) Committee and Plenary, Nov. 19, 2024
Adopted by the Innovation, Cybersecurity, and Technology (H) Committee, Nov. 19, 2024

2025 Proposed Charges

INNOVATION, CYBERSECURITY, AND TECHNOLOGY (H) COMMITTEE

The mission of the Innovation, Cybersecurity, and Technology (H) Committee is to: 1) provide a forum for state insurance regulators to learn about and have discussions regarding: cybersecurity, innovation, data security and privacy protections, and emerging technology issues; 2) monitor developments in these areas that affect the state insurance regulatory framework; 3) maintain an understanding of evolving practices and use of innovation technologies by insurers and producers in respective lines of business; 4) coordinate NAIC efforts regarding innovation, cybersecurity and privacy, and technology across other committees; and 5) make recommendations and develop regulatory, statutory, or guidance updates, as appropriate.

Ongoing Support of NAIC Programs, Products, or Services

1. The **Innovation, Cybersecurity, and Technology (H) Committee** will:
   A. Provide forums, resources and materials related to developments and emerging issues in innovation, cybersecurity, data privacy, and the uses of technology in the insurance industry in order to educate state insurance regulators on these developments and how they affect consumer protection, insurer and producer oversight, marketplace dynamics, and the state-based insurance regulatory framework.
   B. Consider and coordinate the development of regulatory guidance and examination standards related to innovation, cybersecurity, data privacy, the use of big data and artificial intelligence (AI) including machine learning (ML) in the business of insurance, and technology, including drafting and revising model laws, white papers, and other recommendations as appropriate.
   C. Oversee the work of the Data Call Study Group to study the enhancement of regulator access to high-quality and timely data allowing for evidence-informed decisions, enhanced supervisory capabilities, and improved efficiency.
   D. Track the implementation of and issues related to all model laws pertaining to innovation, technology, data privacy, and cybersecurity, including the *Insurance Data Security Model Law* (#668), the *NAIC Insurance Information and Privacy Protection Model Act* (#670), the *Privacy of Consumer Financial and Health Information Regulation* (#672), and the *Unfair Trade Practices Act* (#880) rebating language and providing assistance to state insurance regulators as needed.
   E. Coordinate and facilitate collaboration with and among other NAIC committees and task forces to promote consistency and efficiency in the development of regulatory policy, education, training, and enforcement materials and tools related to innovation; cybersecurity; data privacy; and the use of technologies, big data, and artificial intelligence (AI), including machine learning (ML), in the business of insurance. Evaluate and recommend certifications, continuing education (CE), and training for regulatory staff related to technology, innovation, cybersecurity, and data privacy.
   F. Follow the work of federal, state, and international governmental bodies to avoid conflicting standards and practices.

2. The **Third-Party Data and Models (H) Task Force** will:
   A. Develop and propose a framework for the regulatory oversight of third-party data and predictive models.
   B. Monitor and report on state, federal, and international activities related to governmental oversight and regulation of third-party data and model vendors and their products and services. Provide recommendations to the Innovation, Cybersecurity, and Technology (H) Committee regarding responses to such activities.

3. The **Big Data and Artificial Intelligence (H) Working Group** will:
   A. Research the use of big data and AI (including ML) in the business of insurance. Proactively communicate findings, and present recommendations to the Innovation, Cybersecurity, and Technology (H) Committee.
   B. Monitor state, federal, and international activities on AI, including working with the Innovation, Cybersecurity, and Technology (H) Committee to: 1) respond to such activities, where appropriate, and 2) address potential impacts on existing state insurance laws or regulations.
   C. Facilitate discussion to consider updates to the regulatory framework for the oversight of the use of AI by insured entities. Provide recommendations to the Innovation, Cybersecurity, and Technology (H) Committee in response to such activities.
      a. Monitor and support adoption of the *Model Bulletin on the Use of Artificial Intelligence Systems by Insurers.*
      b. Monitor and report on state, federal, and international activities related to governmental oversight and regulation of the use of AI in insurance and non-insurance industries.
      c. Research, identify, and monitor the impacts of the use of AI systems by insurance companies to understand the potential benefits, value propositions, risks, and adverse consumer outcomes related to the use of AI systems.
   D. Facilitate discussion related to AI systems evaluation including:
      i. Identifying existing tools, resources, materials, and training that will assist and guide regulators in their review of AI systems used by licensees, including an insurer's AI program. This includes establishing a coordinated work plan and timeline for further development of those resources.
      ii. Develop new regulatory tools or regulatory guidance to assist regulators in their review of AI systems used by licensees, including an insurer's AI program.
      iii. Coordinate the development of review and enforcement tools, resources, guidelines, and training related to AI systems for regulators across the NAIC.
   E.
   F. Facilitate and coordinate foundational and contextual educational content for regulators on topics related to the use of big data and AI techniques, tools and systems in the insurance industry.

4. The **Cybersecurity (H) Working Group** will:
   Cybersecurity Charges
   A. Monitor cybersecurity trends such as vulnerabilities, risk management, governance practices, and breaches with the potential to affect the insurance industry.
   B. Facilitate communication across state insurance departments regarding cybersecurity risks and events.
   C. Develop and maintain regulatory cybersecurity response guidance to assist state insurance regulators in the investigation of national insurance cyber events.
   D. Monitor federal and international activities on cybersecurity engaging in efforts to manage and evaluate cybersecurity risk.
   E. 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.
   F. Advise NAIC staff on the development of cybersecurity training for state insurance regulators.

G. Work with the Center for Insurance Policy and Research (CIPR) to receive updates on cybersecurity research efforts, by the CIPR and others, and to analyze publicly available cybersecurity-related information.
H. Support the states with implementation efforts related to the adoption of the *Insurance Data Security Model Law* (#668).
I. Coordinate with NAIC staff to facilitate intelligence-driven cybersecurity tabletop exercises with states departments of insurance (DOIs) providing input on scope and timing as necessary.

Cyber Insurance Charges

A. Monitor industry trends pertaining to cyber insurance, including meeting with subject matter experts (SMEs) and evaluating data needs of state insurance regulators. Considerations should include the availability and affordability/pricing of cyber insurance, disclosures, limits and sub-limits in policies, policy language and trends in requirements, underwriting practices, and the role of reinsurance in the cyber insurance market.
B. Coordinate with NAIC work groups addressing cyber insurance related issues, such as the Casualty Actuarial and Statistical (C) Task Force.
C. Monitor federal and international activities related to cyber insurance and financing mechanisms for cyber risk.
D. Coordinate with NAIC staff to conduct analysis pursuant to the NAIC's Cyber Insurance Report. Review the NAIC's *Property & Casualty Annual Statement Cybersecurity and Identity Theft Supplement* recommending changes and/or developing reports to supplement data development as necessary. Consider and develop a guide for states on cyber insurance data analysis best practices.

5. The **Privacy Protections (H) Working Group** will:
   A. Use state insurance privacy protections regarding the collection, data ownership and use rights, and disclosure of information gathered in connection with insurance transactions to draft a new/revised Privacy Protections Model Act to replace/update NAIC models such as Model #670 and/or Model #672.
   B. Monitor state, federal, and international activities on privacy, engaging in efforts to manage and evaluate privacy.

6. The **SupTech/GovTech Subgroup** will:
   A. Facilitate technology, innovation, and SupTech/GovTech presentations from leading technology companies for state insurance regulators to provide them with insights into cutting-edge technology and innovation.
   B. Facilitate technology, innovation, and SupTech/GovTech presentations from specialized vendors for state insurance regulators to assist in identifying vendor solutions that may benefit regulators.

SharePoint/Support Staff Hub/Member Meetings/H Cmte/2024 Fall/H-Charges2025/_033_H-Cmte-2025-Proposed-Charges-Final.docx

