INNOVATION, CYBERSECURITY, AND TECHNOLOGY (H) COMMITTEE

Innovation, Cybersecurity, and Technology (H) Committee March 18, 2024, Minutes
- Big Data and Artificial Intelligence (H) Working Group March 16, 2024, Minutes (Attachment One)
- Cybersecurity (H) Working Group March 17, 2024, Minutes (Attachment Two)
  - Cybersecurity Event Response Plan (CERP) (Attachment Two-A)

Draft Pending Adoption

Draft: 4/1/24

Innovation, Cybersecurity, and Technology (H) Committee
Phoenix, Arizona
March 18, 2024

The Innovation, Cybersecurity, and Technology (H) Committee met in Phoenix, AZ, March 18, 2024. The following Committee members participated: Kathleen A. Birrane, Chair (MD); Chlora Lindley-Myers, Co-Vice Chair, and Cynthia Amann (MO); Kevin Gaffney, Co-Vice Chair (VT); Ricardo Lara (CA); Michael Conway (CO); Karima M. Woods (DC); Michael Yaworsky (FL); Gordon I. Ito and Lisa Zarko (HI); Dana Popish Severinghaus represented by Erica Weyhenmeyer (IL); Doug Ommen and Daniel Mathis (IA); Jon Godfread (ND); Judith L. French and Tom Botsko (OH); Michael Humphreys (PA); and Alexander S. Adams Vega (PR). Also participating were: Lori K. Wing-Heier (AK); Alan McClain (AR); Wanchin Chou (CT); Stephen C. Taylor (DE); Amy L. Beard and Victoria Hastings (IN); Tom Travis (LA); Phil Vigliaturo (MN); Eric Dunning (NE); Christian Citarella (NH); and Elizabeth Kelleher Dwyer (RI).

1. Adopted its 2023 Fall National Meeting Minutes

Director Lindley-Myers made a motion, seconded by Commissioner Gaffney, to adopt the Committee's Dec. 1, 2023, minutes (*see NAIC Proceedings – Fall 2023, Innovation, Cybersecurity, and Technology (H) Committee*). The motion passed unanimously.

2. Adopted its Task Force and Working Group Reports

A. Third-Party Data and Models (H) Task Force

Commissioner Conway reported that the Third-Party Data and Models (H) Task Force met March 16. During this meeting, it discussed the Florida Hurricane Commission's oversight process for reviewing hurricane models. The Task Force will continue to see what types of regulatory models exist that can potentially be used to build out a framework in the second year of the Task Force's operation.

B. Big Data and Artificial Intelligence (H) Working Group

Commissioner Gaffney reported that the Working Group met March 16. During this meeting, the Working Group discussed its work plan, which includes: 1) collaboration with the Center for Insurance Policy and Research (CIPR) and NAIC staff to continue existing artificial intelligence (AI)/machine learning (ML) survey work; and 2) the commencement of the health AI/ML survey. Additionally, the Working Group discussed project plans, including an update on the NAIC Bulletin adoption tracking process from Holly Weatherford (NAIC). The Working Group and NAIC staff intend to provide further updates on the NAIC website on the adopting states. The Working Group also heard a presentation from Dorothy Andrews (NAIC) on a survey of research activities that the American Academy of Actuaries (Academy) and the Society of Actuaries (SOA) conducted related to bias.

C. Cybersecurity (H) Working Group

Amann reported that the Working Group met March 17. During this meeting, the Working Group took the following actions: 1) adopted the Cybersecurity Event Response Plan (CERP); 2) heard a presentation from the Academy detailing its Cyber Risk Toolkit; and 3) heard a presentation from CyberAcuView, which was related to its data in the spaces of cybersecurity and cyber insurance. The Working Group also discussed its work plan for 2024. Three big topics anticipated are: 1) its work on data collection; 2) its discussion of cyber coverage and cybersecurity; and 3) its planned presentations for this year.

D. E-Commerce (H) Working Group

Director French reported that the Working Group exposed the E-Commerce Modernization Guide for a 30-day regulator-only comment period that ended Feb. 6. NAIC staff received comments and made the necessary changes to the guide. NAIC staff met with the Working Group leadership to review the edits to the guide and discuss the work plan for 2024. The Working Group met in regulator-to-regulator session March 5, pursuant to paragraph 6 (consultations with NAIC staff related to NAIC technical guidance) of the NAIC Policy Statement on Open Meetings, to discuss its work plan for the year. The Working Group exposed the guide for a 30-day public comment period that ended March 14. The Working Group plans to meet April 4 to consider adoption of the guide.

E. Technology, Innovation, and InsurTech (H) Working Group

Director Dunning reported that the Working Group plans to meet in person at the next two national meetings. At the Summer National Meeting, it plans to have a speaker from a broad InsurTech-related focus. For the Fall National Meeting, the Working Group will also look at InsurTech-related issues, with a speaker tied largely to Denver, CO, where the meeting will be taking place.

F. Privacy Protections (H) Working Group

Commissioner Beard reported that the Working Group met March 8 in regulator-to-regulator, pursuant to paragraph 3 of the NAIC Policy Statement on Open Meetings as the regulatory discussion included feedback received from specific companies. During this meeting, the Working Group received a brief presentation from the NAIC on the history of the NAIC privacy models, a review of the Working Group's work over the past several years, and an update on the state privacy law landscape. With the transition of leadership, the Working Group has paused work for the moment on the *Insurance Consumer Privacy Protections Model Law* (#664), but the public continues to show strong interest in privacy-related discussions.

The Working Group will begin holding open meetings with subject matter experts (SMEs) in April to advance the discussion of the issues to be considered by the Working Group. The Working Group intends to schedule open meetings to allow for industry and consumer groups' input on Model #664. In addition, the NAIC Legal team will create an issue matrix, which aggregates the insights from the SMEs and allows for comparison between the last exposure draft, as well as comparisons against the *NAIC Insurance Information and Privacy Protection Model Act* (#670), the *Privacy of Consumer Financial and Health Information Regulation* (#672), and any other relevant drafts. The matrix will be used to understand the central issues and provisions in Model #664, and then the Working Group will continue to hold SME open meetings as necessary, as well as regulator-to-regulator sessions, to determine the best privacy regime and draft a model law that reflects that.

The Working Group intends to move forward with a focus on consensus building among members, industry, consumer groups, and fellow state insurance regulators, as well a focus on transparency.

G. Other Meetings

Commissioner Godfread reported that the Data Call Collaboration Forum is in process of building on its project in North Dakota on blockchain. He said it is also moving forward with a discussion at the NAIC level regarding how state insurance regulators collect and analyze data, which will eventually include a discussion on data standardization.

Commissioner Ommen reported that the AI Systems Evaluation and Training Collaboration Forum met March 17 in regulator-to-regulator session and had a good discussion with members from several working groups and from the Market Regulation and Consumer Affairs (D) Committee. The work will advance the discussion on how AI

systems are evaluated, with recommendations eventually coming back to the Committee to move forward on the topic.

Commissioner Birrane noted that the Committee met earlier this morning in regulator-to-regulator session, pursuant to paragraph 3 (specific companies, entities, or individuals) of the NAIC Policy Statement on Open Meetings, with the consumer representatives. The Committee has committed to having a regulator-to-regulator discussion with the consumer representatives in person at every national meeting going forward, and it will have virtual meetings in between to ensure it receives input throughout the process.

Commissioner Gaffney made a motion, seconded by Commissioner Lara, to adopt the reports of the Third-Party Data and Models (H) Task Force; Big Data and Artificial Intelligence (H) Working Group (Attachment One); the Cybersecurity (H) Working Group (Attachment Two); the E-Commerce (H) Working Group; the Technology, Innovation, and InsurTech (H) Working Group; the Privacy Protections (H) Working Group; and the Collaboration Forums. The motion passed unanimously.

3. Heard a Presentation from Uber on Working with AI and ML

Frank Chang (Uber and Casualty Actuarial Society—CAS) introduced telematics as an example of an advanced application of AI and ML. He explained how telematics, leveraging smartphone sensors, detects driving events such as measuring distance for usage-based insurance and identifying crashes. Through telematics, insurers can assess risk more accurately and incentivize safer driving behaviors among policyholders. He discussed the evolving landscape of advanced driver assistance systems (ADAS) and its implications for insurance modeling, such as the complexities of incorporating factors for lane change assist (LCA) and possible ensuing behavioral impacts of these features.

Chang raised possible concerns about overall data quality and modeling, and he emphasized the need for thorough validation to ensure the reliability of model outputs. He discussed the issue of fairness in insurance pricing, noting the potential biases that may be inherent in telematics data analysis. He also discussed the three approaches to achieving fairness in pricing—omission, equal rates, and equalized odds—and highlighted the considerations involved in each of these approaches.

Chang transitioned to discussing the use of large language models (LLMs) in insurance and offered insights into their respective strengths and weaknesses. He discussed major security vulnerabilities of LLMs by providing examples of prompt injection attacks that can cause the systems to bypass their intended constraints, specific exploits such as the "dead grandmother" trick, and real-world incidents where chatbots misrepresented companies' product pricing policies. To mitigate such risks, he recommended governance protocols such as human monitoring of chatbot conversations, data sanitation to block malicious prompts, circuit breakers to disable compromised bots, and understanding an AI system's limitations upfront.

Commissioner Birrane asked Chang about his thoughts on proper governance oversight of LLMs used in insurance. Chang replied that if LLMs offer help or support with no financial consequences, then testing can be performed a little more lightly. However, if LLMs are used for binding a policy or filing a claim, then stronger monitoring for exploits would be required.

Miguel Romero (NAIC) asked whether there are any more specific guidelines or metrics to judge the amount of data needed for the complexity of a model. Chang responded that actuaries have credibility standards for loss data. He also said there are statistical tests such as Akaike information criterion (AIC) and Bayesian information criterion (BIC) that can be performed to estimate whether an extra variable included in a model provides significant predictive value. In the validation of a model, use a hold-out sample or k-fold cross-validation sampling to test performance.

Citarella asked whether data scientists consider telematics data collected in the context where the human is assisted with an ADAS device, such that the driver is not always taking the preventive action. Chang responded that it is important to recognize whether rating factors indicated from telematics data and rating factors indicated from vehicle characteristics are not double-counted.

Chou remarked that state insurance regulators want to encourage accuracy, but they are also concerned about consumer protection. He asked how regulators can be sure a model used by an insurer is accurate. Chang responded that regulators should start by asking the easy, more obvious questions to perform first-level human validation and then dig deeper by performing a review of the model predictions for a sample of policies.

Vigliaturo asked whether the severity of losses is also considered along with the frequency of claims, and he remarked that having an ADAS device might make a driver less vigilant. Chang responded that severity is also taken into account in insurance modeling of telematics data and that there is quite a bit of literature that talks about human brains "shrinking" from the use of GPS maps as compared to reading a physical printed map. However, he said he is not aware of this phenomenon in response to the usage of ADAS in vehicles.

4. Heard an Update on Federal Activities Related to AI

Shana Oppenheim (NAIC) noted that proposed bills by Congress aim to address various aspects of AI, from financial risk to transparency, governance, and environmental impacts. Oppenheim said that Sen. Mark Warner (D-VA) and Sen. John Kennedy (R-LA) have introduced legislation that would require the Financial Stability Oversight Council (FSOC) to coordinate a response to market stability threats posed by AI, such as the use of deepfakes, and recommend ways to close regulatory gaps. The bill would also allow the U.S. Securities and Exchange Commission (SEC) to pursue penalties for market manipulation and fraud involving AI, and it would give credit unions and housing regulators authority to oversee AI service providers.

The federal AI Foundation Model Transparency Act directs the Federal Trade Commission (FTC), along with the National Institute of Standards and Technology (NIST) and the White House Office of Science and Technology Policy (OSTP), to create standards for transparency in training data and algorithms used in AI tools. Companies creating AI tools would be required to share with consumers and regulators data on how models are trained, mechanisms used for training, and possible collection of data. The AI Governance and Transparency Act encourages the responsible use of AI in agencies and offers guidance on implementation.

Lastly, the Artificial Intelligence Environmental Impacts Act of 2024, introduced by Sen. Edward J. Markey (D-MA), Sen. Martin Heinrich (D-NM), Rep. Anna Eshoo (D-CA), and Rep. Don Beyer (D-VA) Beyer, aims to measure and report the full range of environmental AI impacts through inter-agency study, as well as create a voluntary framework for developers to report environmental impacts.

Oppenheim reported that the bipartisan AI Committee Working Group announced by Rep. Maxine Waters (D-CA) is led by the Digital Assets, Financial Technology, and Inclusion Subcommittee, and Chair French Hill (R-AR) also plans to explore the impact on financial services and housing industries, including fraud, prevention, and compliance efficiency. Oppenheim also noted there is a bipartisan Task Force on Artificial Intelligence that was announced by U.S. House of Representatives Speaker Mike Johnson and Rep. Hakeem Jeffries (D-NY), which is aimed at ensuring the U.S. continues to lead in AI innovation while considering guardrails that may be appropriate to safeguard the nation. The U.S. Government Accountability Office (GAO) has identified several areas of AI concern, including natural hazard modeling using AI, and it has issued a report outlining 35 recommendations to address the issue that there is no government-wide guidance for agencies implementing AI themselves. The FTC and the Commodities Futures Trading Commission (CFTC), as well as the National Telecommunications and

Information Administration (NTIA), are also looking into the use of AI in their regulated entities and in their own usage.

Finally, Oppenheim reported that the White House has an AI council that is working to develop safe, secure AI model standards. The AI council is convened by the deputy chief of staff, as well as several leading Artificial Intelligence Safety Institute Consortium (AISIC) members, including Microsoft, Meta, and Google, which are among 200 members of this newly established AI Safety Institute Consortium under the Department of Commerce, as well as the National Institute of Standards and Technology.

5. Heard a Presentation from DLA Piper on International Activities Related to AI

Danny Tobey (DLA Piper) covered various aspects of AI regulation and governance. He outlined the broad scope of the discussion, touching upon how state insurance regulators are examining the regulation of AI not only within the insurance sector, but also across other industries. He highlighted the European Union's (EU's) recent legislative developments and reflected on recent developments in AI governance. He also highlighted 2023 and 2024 as significant watershed years, noting the insurance sector's proactive stance on addressing AI-related issues and how other industries like employment, health care, and finance are ramping up enforcement efforts as well.

Tobey noted AI-specific regulatory actions taken by the Federal Trade Commission (FTC) focused on the value chain of development, or the AI stack, from the foundation model developers to the customizers/fine-tuners, adopters, and through the consumers who use the models. The FTC uses an accountability matrix because the skill sets are spread across layers of development in an organization, and it has imposed penalties for algorithmic manipulation and actions against misleading AI disclosures in corporate settings. This can include algorithmic disgorgement. The U.S. Department of Justice (DOJ) has brought criminal actions against those who overpromised their AI capabilities. The SEC has also been active in regulating AI. Tobey noted currently proposed state legislation in Kentucky, Louisiana, New Jersey, and Washington that provides for consumer disclosures and control over their personal/biometrics data and how it is used.

Tobey discussed various legal aspects of potential harms from wide horizontal risks, including the implications of AI for product liability and tort claims. He mentioned specific cases such as copyright disputes and employment discrimination claims, along with the evolving legal considerations for AI inventions and patents. He then provided more information on the EU's Artificial Intelligence Act (AI Act), emphasizing its risk-based approach and extraterritorial applicability. Additionally, he discussed the AI Act's categories of risk and potential impacts on companies operating within and outside the EU. He also highlighted proposed acts, bills, and regulatory legislation introduced in other countries, largely guided by what the EU has done. He noted that the common denominator is pre- and post-implementation testing, especially in high-risk sectors, and he acknowledged the ongoing academic and industry collaboration in shaping regulatory methodologies.

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

SharePoint/NAIC Support Staff Hub/Member Meetings/H Cmte/2024_Spring/H-Minutes/H-Cmte-Minutes031824.docx

Draft: 4/4/24

Big Data and Artificial Intelligence (H) Working Group
Phoenix, Arizona
March 16, 2024

The Big Data and Artificial Intelligence (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Phoenix, AZ, March 16, 2024. The following Working Group members participated: Kevin Gaffney, Chair (VT); Michael Humphreys, Vice Chair (PA); Mark Fowler (AL); Tom Zuppan (AZ); Ken Allen and Mitra Sanadajifar (CA); Michael Conway and Carol Matthews (CO); George Bradner and Wanchin Choy (CT); Rebecca Smid (FL); Andrew Hartnett (IA); Weston Trexler (ID); Erica Weyhenmeyer and Shannon Whalen (IL); Victoria Hastings (IN); Shawn Boggs (KY); Tom Travis (LA); Caleb Huntington, Rachel M. Davison, and Jackie Horigan (MA); Kathleen A. Birrane (MD); Sandra Darby (ME); Tina Nacy (MI); Phil Vigliaturo (MN); Cynthia Amann (MO); Tracy Biehn and Angela Hatchell (NC); Colton Schulz (ND); Christian Citarella (NH); Justin Zimmerman (NJ); Nick Stosic and Hermoliva Abejar (NV); Sumit Sud (NY); Judith L. French, Matt Walsh, and Rodney Beetch (OH); Landon Hubbart (OK); TK Keen (OR); Elizabeth Kelleher Dwyer (RI); Michael Wise and Will Davis (SC); Travis Jordan (SD); Emily Marsh (TN); J'ne Byckovski and Randall Evans (TX); Scott A. White, Eric Lowe, and Michael Peterson (VA); Bryon Welch (WA); Nathan Houdek (WI); Allan L. McVey (WV); and Jeff Rude (WY). Also participating was: Trinidad Navarro (DE).

1. Adopted its 2023 Fall National Meeting Minutes

Commissioner Humphreys made a motion, seconded by Commissioner Birrane, to adopt the Working Group's Dec. 1, 2023, minutes (*see NAIC Proceedings – Fall 2023, Innovation, Cybersecurity, and Technology (H) Committee, Attachment Two*). The motion passed unanimously.

2. Discussed its Project Plans for 2024

Commissioner Gaffney discussed the Working Group's project plan for 2024. He noted that although specific timelines were noted, in some cases, the timelines should be treated as estimates to allow for flexibility. Commissioner Gaffney introduced each project by first citing the relevant Working Group charges.

The projects relevant to the charge of "researching the use of big data, AI/ML in insurance—communicate findings and present recommendations to the H Committee" include: 1) collaborating with the Center for Insurance Policy and Research (CIPR) to perform additional analysis of the artificial intelligence (AI)/machine learning (ML) survey results; 2) comparing survey results to the bulletin to identify areas where it can be improved or where additional follow-up with industry should be considered; and 3) developing the health insurance AI/ML survey, considering a plan for continued survey work.

Commissioner Gaffney noted that the development group has convened with representatives from 17 states (Colorado, Connecticut, Illinois, Iowa, Louisiana, Maryland, Michigan, Minnesota, Nebraska, North Dakota, Oklahoma, Oregon, Pennsylvania, Vermont, Virginia, West Virginia, and Wisconsin) to develop the AI/ML health survey. Further, he noted that the health insurance products to include in the survey were narrowed down to comprehensive major medical (individual and group), student health plans, limited benefit plans, and stop loss/excess loss plans and that, as with previous surveys, the Working Group will plan to engage with companies in a pilot study of the survey to solicit feedback on the initial survey design. These meetings will be one-on-one, regulator-to-regulator meetings. Results are anticipated to be reported by the 2024 Summer National Meeting.

Commissioner Gaffney stated the Working Group will also work concurrently to hold regulator-to-regulator sessions with selected private passenger auto (PPA) companies to get an update on their AI/ML activities since completing the auto survey about two years ago and talked about developing updated surveys that can be issued periodically to stay abreast of industry uses of AI/ML in their operations.

The projects relevant to the charge of "monitoring and responding to state, federal, and international activities on AI to address impacts on insurance laws or regulations" include: 1) receiving a report from the volunteer group comparing the model bulletin to the White House Executive Order; and 2) continuing to receive federal and international updates on AI.

The projects relevant to the charge of "overseeing the work of the Collaboration Forum on Algorithmic Bias" include: 1) tracking adoption of the model bulletin; and 2) developing a reference glossary/lexicon. Commissioner Gaffney noted that the discussions on the initiative to create an independent synthetic dataset are tabled for the time being, pending resource planning and working through logistical issues and that this project will be revisited in the future as other projects take shape.

Holly Weatherford (NAIC) provided an update on the adoption of the model bulletin. In her update, she noted that the NAIC has created a model bulletin state adoption map that will be posted to the Working Group's web page in the next week or so and will be updated monthly. As an update, six states have adopted the model bulletin in less than three months. Weatherford said the NAIC also acknowledges action that was taken by two states prior to the model bulletin's adoption, which issued guidance or adopted a specific law or regulation. The NAIC is performing a deeper dive that will go into more detail about how states have adopted the model bulletin and will provide a quick reference grid as a guide that tracks it as well. Weatherford concluded by stating that the NAIC is looking into providing another tool to help guide state insurance regulators through the drafting of the model bulletin, taking into consideration industry comments that were provided throughout its development.

Commissioner Gaffney concluded that the Working Group plans to have additional coordinating discussions on the projects relevant to the charge of "coordinating educational content for regulators on Big Data and AI in insurance," pending the advancement of the Innovation, Cybersecurity, and Technology (H) Committee's related initiatives to avoid duplication of effort.

Commissioner Gaffney then invited discussion on the work plan from Working Group members, interested state insurance regulators, and interested parties.

Peter Kochenburger (Southern University Law Center, NAIC Consumer Representative) asked why the information about the adoption of the model bulletin will be kept in a regulator-only setting. Commissioner Gaffney clarified that this information will be made public. Kochenburger expressed the need to provide specific consumer protections and requirements beyond the high-level principles set forth in the model bulletin.

Scott Harrison (American InsurTech Council) asked whether the AI/ML health survey will include natural language processing (NLP) or robotic processing automation (RPA). He said the concern is that the survey should include the full scope of what is currently being used by insurance companies. Commissioner Gaffney acknowledged that concern.

3. Heard a Presentation on a Survey of Research Activities Conducted by the Academy and the SOA Related to Big Data, AI, Fairness, Bias, and Governance

Dorothy Andrews (NAIC) discussed the development of a list of technical papers and a webinar from the American Academy of Actuaries (Academy) on the issues of bias, explained possible sources of bias, the general problems associated with data biases, AI, how AI unfairness could happen, how to test for bias, and a framework for evaluating an analysis of bias. She highlighted some of the questions raised during the panel presentation, including inquiries about the definition of big data, methods to avoid bias, the difference between data scientists and analysts, and the importance of including social scientists in discussions about algorithmic accountability.

Andrews discussed various types of bias, such as sample bias, label bias, model pipeline bias, and application bias, and the challenges associated with measuring and addressing them. She emphasized the importance of considering fairness metrics and tests when evaluating bias in AI models and noted the Academy is working to address these questions and working on papers about algorithmic auditing for bias and political bias in pension evaluations. She also mentioned a presentation on property and casualty bias by the Academy and the need for an increased understanding of AI bias concepts within the profession.

In addition, Andrews noted other initiatives from the National Institute of Standards and Technology (NIST) and the International Actuarial Association (IAA) to set standards and provide education on AI governance and shared her involvement in various research initiatives, including a study on consumer awareness of third-party data used in auto insurance premiums, and her Ph.D. work on social justice issues in auto insurance rating. Andrews acknowledged the ongoing need for education and awareness around bias in AI within the regulatory and professional communities.

4. Received an Update on International Developments on AI/ML in Insurance

Ryan Workman (NAIC) highlighted the involvement of the NAIC and state insurance regulators in international efforts concerning AI/ML, including participation in the International Association of Insurance Supervisors (IAIS) FinTech Forum and the Organisation for Economic Co-operation and Development (OECD) Insurance and Private Pensions Committee (IPPC) workstream on AI. Workman noted that the AI/ML subgroup of the IAIS FinTech Forum conducted a thematic review of existing guidance on AI/ML and model risk management from 12 supervisory authorities and international organizations, including the NAIC, which aimed to facilitate the exchange of supervisory practices and experiences, particularly in addressing potentially new or heightened risks associated with AI/ML. Further, the NAIC will contribute to the upcoming development of an IAIS application paper on AI/ML in 2024 and continue participating in IAIS FinTech-related discussions and developments, including discussions on emerging trends in SupTech.

Workman also noted the establishment of the Innovation and Technology Working Group within the EU-U.S. Insurance Dialogue Project, in which members discuss the relationship between innovation, technology, and insurance, specifically the increasing use of advanced data analytics in the insurance sector, including the benefits and concerns related to AI/ML in pricing and underwriting. The use of new technology and large datasets in pricing and underwriting may potentially lead to excessive segmentation of the risks, unfair/unlawful price discrimination, overreliance on third-party vendors, and the inability to verify data accuracy.

Workman summarized recent discussions within the workstream, including topics on appropriate regulatory frameworks for AI/ML in insurance governance and impact on historically underrepresented groups, and concluded by mentioning that discussions on regulatory developments such as the NAIC AI model bulletin and the EU AI Act will continue in 2024.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Spring/WG-BDAI/Spring-Minutes/Minutes-BDAIWG031624-Final.docx

Draft: 4/2/24

Cybersecurity (H) Working Group
Phoenix, AZ
March 17, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Phoenix, AZ, March 17, 2024. The following Working Group members participated: Cynthia Amann, Chair, and Brad Gerling (MO); Michael Peterson, Vice Chair (VA); Chris Erwin (AR); Wanchin Chou (CT); Daniel Mathis (IA); Ryan Gillespie and Erica Weyhenmeyer (IL); Craig VanAalst (KS); Kory Boone (MD); Jeff Hayden (MI); T.J. Patton (MN); Colton Schulz (ND); Christian Citarella (NH); David Cassetty and Nick Stosic (NV); Avani Shah/Sumit Sud (NY); Matt Walsh (OH); John Haworth (WA); and Tim Cornelius and Rebecca Rebholz (WI). Also participating was: David Buono (PA).

1. Adopted its 2023 Fall National Meeting Minutes

Haworth made a motion, seconded by Peterson, to adopt the Working Group's Nov. 16, 2023, minutes. (*see NAIC Proceedings – Fall 2023, Cybersecurity Insurance (H) Working Group, Attachment Three*). The motion passed unanimously.

2. Adopted the Cybersecurity Event Response Plan (CERP)

Amann recognized Peterson for spearheading the Cybersecurity Event Response Plan (CERP) and Rabin for working with Peterson on the document. She said the CERP is intended to be guidance for departments of insurance (DOIs) when they must respond to a cybersecurity event. The plan will also help new DOI employees understand the response process. If a state has adopted its own version of the NAIC *Insurance Data Security Model Law* (#668), the information in the guidance will need to be updated to comply with the state's law. Additionally, states can change the document information to meet their needs. The document includes topics such as communication among various stakeholders, understanding and receiving notifications, required information that needs to be provided to a DOI, and a process that can be used to respond to cybersecurity events defined in the Model #668. The document also includes a sample template that can be used by a DOI when requesting information from the breached party. The Working Group worked closely with interested parties to incorporate their suggestions into the CERP. The document was exposed twice, and suggested changes were made where applicable.

Peterson made a motion, seconded by Haworth, to adopt the CERP (Attachment Two-A). The motion passed unanimously.

3. Heard a Presentation from the Academy on its Cyber-Risk Activities

Richard Gibson (American Academy of Actuaries—Academy) gave an informational presentation to the Working Group. The Academy is the only U.S.-based actuarial organization solely focused on serving the public and the entire actuarial profession. The Academy encompasses all practice areas and ensures the profession's ability to self-regulate by housing the actual board for counseling and disciplining, the joint committee on the code of professional conduct, and the committee on qualifications. Chou is the chairperson of the committee on cyber risk.

The Academy is engaged in public policy issues. The Academy's Casualty Practice Council (CPC) is the umbrella committee for major property/casualty (P/C) insurance issues. The CPC provides objective technical expertise to policymakers and regulators. The Academy does not work for insurers or regulators. The Academy has a committee on cyber risk that monitors the actual aspects of cyber risk. There are more than 20 members on this team, all of which are volunteers. A majority of the volunteers on the committee are working in cyber on a regular basis.

The Academy has been working on a cyber risk toolkit for the last three to four years and continues to update the toolkit on a regular basis. The toolkit includes papers that address issues pertinent to cyber risk and exposures that are now impacting most lines of business. Cyber exposure extends to many other coverages. Each part of the toolkit is a standalone paper, but it provides a cohesive overview of the challenges posed in the cyber insurance market. The cyber insurance market is constantly evolving with respect to new threats, new coverages, and new crises. The toolkit will be updated periodically to reflect new and emerging work from the Cyber Risk Committee.

The key papers within the Cyber Risk Toolkit include *An Introduction to Cyber*; *Cyber Threat Landscape*; *Silent Cyber*; *Cyber Data*; *Cyber Risk Accumulation*; *Cyber Risk Reinsurance Issues*; *Ransomware*; *War, Cyberterrorism, and Cyber Insurance*; *Autonomous Vehicles and Cyber Risk*; *Personal Cyber: An Intro to Risk Reduction and Mitigation Strategies*; *Digital Assets and Their Current Roles Within Cyber Crime*; and *Cyber Risk Resource Guide*.

The Cyber Risk Committee is currently in the process of a cyber vendor model review. While the committee is not able to review all of the existing cyber models, it is trying to get a sense of how cyber models are working and how they are evolving. The Academy is not endorsing models but trying to understand the parameters and the output they provide, as well as the model's usefulness.

The Cyber Risk Committee is also working on an outline for international cyber considerations and delving deeper into cyber personal lines insurance and the rating on the personal lines side of cyber insurance. An outline about cyber insurance and directors and officers (D&O) coverage is also in the works. In 2020, the Academy published a report on cyber breach reporting requirements, which provides an analysis of laws across the U.S. This document can be found on the Academy's website.

The Academy is working with a business school in Paris, France, to estimate the economic value of cyber risk. The methods being used consider both the heavy-tailed distribution of extreme events and the rapid changes in the underlying hazard. The hope is to get access to the Federal Bureau of Investigation's (FBI's) database on cyber events so work can move forward and be reproduced for the U.S. The Working Group will continue its interaction with the Academy.

4. Heard a Presentation from CyberAcuView About its Organization

Monica Lindeen (CyberAcuView) said the cyber-insurance market continues to mature. Following a health care data breach in 2015, the cyber-insurance market began to harden. In 2016 and 2017, a lot of new carriers entered the cyber-insurance market, and coverage began expanding. While 2018 and 2019 saw lower rates, ransomware severity increased.

CyberAcuView was created by insurance industry leaders, and the organization acts as a thought leader on issues surrounding cyber insurance. CyberAcuView was formed to help increase innovation and competition in the cyber-insurance market and to help combat the increasing threat of cyberattacks. Since CyberAcuView's establishment, it has been working to help insurers provide better value and service to its policyholders and their cyber-risk

mitigation. The organization also has been helping to provide leadership in fighting cybercrime to improve resilience to cyber risk, as well as helping to ensure a competitive cyber-insurance market. CyberAcuView believes the cyber-insurance market will continue to mature with access to experience data, stronger underwriting, capital market investments, the development of cyber definitions and standards, engagement with law enforcement, and collaboration of systemic resolutions that will benefit both the policyholders and society.

Mark Camillo (CyberAcuView) said the core reason for CyberAcuView being formed was data aggregation. There are currently more than 20 members that participate in CyberAcuView, which represents approximately 60% of the cyber-insurance market. However, not everyone in the market reports data. Prior to the formation of CyberAcuView, there was not a platform that insurers had to benchmark how they were performing against their peers and how their loss ratios were looking in various industries and segments. CyberAcuView began to collect and aggregate data. CyberAcuView's collection of the data and aggregation provides a benchmark to insurers. On a quarterly basis, claims data is aggregated, anonymized, and provided to CyberAcuView's members. To get data out of the pool, the insurer must provide data, as the data services are voluntary. CyberAcuView enables insurers to retain the value of their own data by being a statistical reporting agent. Statistical reporting services are available in all states, as required.

CyberAcuView is also working on cyber-data standards. It developed an incident response claims taxonomy for both cyber exposures and cyber claims data. CyberAcuView also publishes standards as an open cyber standard that is governed by CyberAcuView and can be accessed and used by all market participants. CyberAcuView has started collecting data in 2019 and has data through the end of the third quarter of 2023. Over 30,000 claims have come in since 2019, and a little over $4 billion in payments, with about $500 million in reserves. Less than one-third of the claims are for ransomware. However, more than half of those losses were actually caused or driven by ransomware. CyberAcuView collects the top ransomware variants in terms of ransomware claims. It also provides information about the industry groups and tracks the number of claims notices.

CyberAcuView runs quarterly workshops to stimulate discussion and help insurers develop a better understanding of events that drive systemic risk. They also discuss how insurers can help the areas of systemic risk, and how to help increase society's resilience to systemic cyber risk. Past workshops have focused on cloud failure and outages, issues confronting cyber insurance-linked securities (ILS)/alternative capital markets, systemic risk extensions that have been introduced in the marketplace, and cyber risk modeling considerations.

Lindeen leads the efforts on regulatory collaboration, acting as a resource for organizations.

Camillo addressed the potential federal cyber backstop. CyberAcuView will continue to evaluate the potential of a federal cyber backstop.

CyberAcuView has a head of law enforcement engagement that works closely with the FBI through its public/private partnership with the National Cyber-Forensics and Training Alliance (NCFTA). The group is developing a pilot program to actively disrupt and seize ransomware payments by coordinating with other technology companies.

CyberAcuView developed a policy form that can be used by market participants to define risks more precisely, remove ambiguities, and attract more capacity into the market. The cyber war exclusion language was accepted and posted to the Legal Marketing Association (LMA) website. Several insurers are currently going through the process of updating their war language and using the CyberAcuView war exclusion language as a template.

CyberAcuView has endorsed the Cybersecurity and Infrastructure Security Agency's (CISA's) bad practices list as a voluntary minimum cybersecurity best practice to improve policyholder security maturity. It also has expanded outside of the U.S., with its first international data call in the United Kingdom (UK) and Canada.

CyberAcuView collaborated with Pan-European Insurance Risks Information System (PERILS) in Europe to create a U.S. cyber loss index to help accelerate the growth of the cyber ILS and industry loss warranty (ILW) markets. PERILS does work similar to CyberAcuView for the European market on the natural catastrophe side.

The only 2023 event CyberAcuView continues to track is the MOVEit vulnerability. Based on the data they were able to gather and collect in the first quarter of 2024, the losses are below the $500 million reporting threshold. CyberAcuView will continue to monitor to see if the cost rises above the threshold. The methodology can be found by visiting https://cyber.perils.org/#methodology.

5. Discussed the Working Group's Work Plan

The Working Group will look at the current *Cybersecurity Supplement* to see what other information might be advantageous to collect. The Working Group also will discuss some of the following issues in the next year:

- The impact of both hardware and software legacy systems.
- Reviewing the European Union's (EU's) recent Artificial Intelligence Act to the extent that it impacts cyber.
- Data modernization and standardization.
- Third-party vendor oversight.
- Educating its fellow regulators and the insurance industry.
- The knowledge among regulators regarding cyber is disparate, so the Working Group will make sure information is being brought to it from experts.
- Two panels at the Insurance Summit.
- One-to-many reporting.
- Ensuring that both small and large businesses are aware of what their cyber coverage actually covers.
- Working with the Information Technology (IT) Examination (E) Working Group.
- Tracking Model #668 adoptions, as well as changes by the states adopting the model law.
- Panels with an insurer, broker, and reinsurer.
- Hearing from the Center for Insurance Policy and Research (CIPR).
- Hearing from CyberCube.

Peterson is a member of the Financial Stability Board (FSB) for discussions about cybersecurity event notifications standardization.

6. Discussed Other Matters

Amann reminded the Working Group of the Working Group's call on March 27.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Spring/WG-Cybersecurity/Minutes-CyberWG031724-Final.docx

CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

Introduction

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

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

Scope

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

Forming a Team and Communicating with Consumers and Licensee Officials

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

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

Communication with Law Enforcement and Other Regulators

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

CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

Understanding and Receiving Notifications and Required Information

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

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

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

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

CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

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

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

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

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

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

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

CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

Process for Responding to Cybersecurity Events

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

- What is known about the compromise, and is there an ongoing threat?
- Is there a greater threat to the insurance industry (e.g. through the involvement of third-party software many insurers use)?
- Has the licensee lost the ability to process transactions? Can they process claims? Premiums?
- Can the licensee communicate with policyholders? Are their telephones, email, and website working?
- Has the licensee engaged in any general communication with policyholders? Is the licensee able to post a notice on its website? If so, when was the notice posted?
- Has law enforcement responded to the licensee's situation? Are they on-site?
- Are there other professionals on-site assisting with the recovery? What are their roles?

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

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

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

- Using the Powers of the Commissioner to examine and investigate and take appropriate enforcement action Under Section 7(A) and (B) described in MDL-668, if adopted and in effect;
- Bringing an investigation via the exam process described in the *NAIC's Financial Condition Examiners Handbook*; and

CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

- Using the following checklists included in the NAIC's *Market Regulation Handbook to assist the DOI's inquiry:*
  - "Insurance Data Security Pre-Breach Checklist," and
  - "Insurance Data Security Post-Breach Checklist"."

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

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

How to Receive Notifications and Acquire Required Information

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

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

CYBERSECURITY EVENT RESPONSE PLAN
CYBERSECURITY (H) WORKING GROUP

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

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