

## **INNOVATION, CYBERSECURITY, AND TECHNOLOGY (H) COMMITTEE**

Innovation, Cybersecurity, and Technology (H) Committee March 22, 2023, Minutes

Big Data and Artificial Intelligence (H) Working Group March 22, 2023, Minutes (Attachment One)

Cybersecurity (H) Working Group March 7, 2023, Minutes (Attachment Two)

Cybersecurity (H) Working Group 2023 Work Plan (Attachment Two-A)

Memorandum to Information Technology (IT) Examination (E) Working Group Dated March 7, 2023, Regarding  
Cybersecurity Procedures (Attachment Two-B)

Privacy and Protections (H) Working Group March 21, 2023, Minutes (Attachment Three)

SharePoint/NAIC Support Staff Hub/Member Meetings/H Cmte/2023\_Spring/H\_Minutes/Contents.docx

## Draft Pending Adoption

Draft: 4/6/23

Innovation, Cybersecurity, and Technology (H) Committee  
Louisville, KY  
March 22, 2023

The Innovation, Cybersecurity, and Technology (H) Committee met in Louisville, KY, March 22, 2023. The following Committee members participated: Kathleen A. Birrane, Chair (MD); Michael Conway, Co-Vice Chair, and Jason Lapham (CO); Doug Ommen, Co-Vice Chair (IA); John F. King (GA); Gordon I. Ito and Lance Hirano (HI); Dana Popish Severinghaus (IL); Chlora Lindley-Myers represented by Cynthia Amann (MO); Troy Downing (MT); Jon Godfread and Chris Aufenthie (ND); Adrienne A. Harris represented by John Finston (NY); Judith L. French (OH); Carter Lawrence (TN); Kevin Gaffney (VT); and Mike Kreidler and Molly Nollette (WA). Also participating were: Lori K. Wing-Heier (AK); George Bradner (CT); Weston Trexler (ID); Amy L. Beard (IN); Sandra Darby (ME); Grace Arnold (MN); Angela Hatchell (NC); Jennifer A. Catechis (NM); Elizabeth Kelleher Dwyer (RI); and Katie Johnson (VA).

### 1. Adopted its 2022 Fall National Meeting Minutes

Director French made a motion, seconded by Commissioner Godfread, to adopt the Committee's Dec. 13, 2022, minutes (*see NAIC Proceedings – Fall 2022, Innovation, Cybersecurity, and Technology (H) Committee*). The motion passed unanimously.

### 2. Adopted the Reports of its Working Groups

#### A. Big Data and Artificial Intelligence (H) Working Group

Superintendent Dwyer said the Big Data and Artificial Intelligence (H) Working Group met March 22 at the Spring National Meeting.

Related to the Working Group's survey efforts, Superintendent Dwyer reported that the home insurance survey is complete, with the Working Group now shifting to the analysis phase of the project. A public report is to be provided to the public at the Summer National Meeting.

Superintendent Dwyer reminded attendees that the private passenger auto (PPA) insurance survey report is already available on the Working Group's website.

Lastly, related to the survey work, the artificial intelligence (AI)/machine learning (ML) life insurance survey is scheduled to be distributed by the end of March. The requesting states intend to issue a public report by the Fall National Meeting.

The Working Group's third-party vendor workstream has three deliverables this year.

First, using the results of the survey work, the workstream will develop a library of third-party vendors operating in the PPA market, home market, and life market. The library will be completed for both the PPA and home markets by the Summer National Meeting. The library for the life market will be delivered by the Fall National Meeting. The second deliverable of this workstream is to develop a regulator-only tool for states to share information about third-party vendors' activities, similar to what the NAIC has developed for states to share information about the review of property/casualty (P/C) rating models. This tool will be available by the end of April. The final deliverable is a set of model and data regulatory questions, which state insurance regulators may use to ask about models and data used by insurance companies. A revised draft of the questions should be circulated by the end of April. Those in the industry have submitted comments raising the following issues: 1) the

## Draft Pending Adoption

document should be principle-based; 2) the document should be more limited in scope to encourage state insurance regulators to focus on higher-risk AI models; 3) questions should be prioritized to recognize the importance of model governance; 4) there are questions about assumptions of law that are not based in law; 5) there are concerns about redundancy with financial examinations and the potential burdens on smaller companies and smaller AI providers; and 6) the document needs to clarify the intended use of the questions.

The third workstream under the Working Group will evaluate tools and resources for monitoring the industry's use of data and AI/ML. This workstream will create a library of tools, metrics, and resources available to the insurance industry for managing AI/ML activity by the Summer National Meeting. The workstream may then pursue a more formal assessment of the strengths and weaknesses of these tools.

The final Working Group workstream, which is addressing the development of a regulatory framework for AI/ML, has not been active due to work on the AI Interpretive Bulletin, which will address regulatory expectations for the use of AI by insurers, as well as regulatory oversight and examination considerations. Related to the final workstream, Commissioner Beard said that the state insurance regulators have started leaning toward the idea of an independent data set, which could help in testing for bias. The work would progress with the assistance of Dorothy L. Andrews (Center for Insurance Policy and Research—CIPR) and the CIPR. Birny Birnbaum (Center for Economic Justice—CEJ) asked who would be responsible for the development of an independent data set and how the project came about. Commissioner Birrane said that the project cannot be elaborated on because, at this point, state insurance regulators have just started to brainstorm the possibilities of the project.

### B. Cybersecurity (H) Working Group

Amann said the Cybersecurity (H) Working Group's most significant project is the planned cybersecurity response plan. The Working Group has volunteers and has drafted an outline document that the volunteers will now meet to expand on. The response plan will serve as an aid to states responding to cybersecurity events occurring at regulated entities. Additionally, the Working Group, as part of its efforts to monitor federal cybersecurity developments, will be having discussions about cloud service providers that insurers are using, whether state insurance regulators should have that data, and how they would go about getting that data. Third, the Working Group will send a referral to the Information Technology (IT) Examination (E) Working Group, asking it to consider updating its guidance based on recent releases by the Cybersecurity and Infrastructure Security Agency (CISA). The Cybersecurity (H) Working Group will also continue to support NAIC training initiatives. Lastly, the Working Group will also be working with NAIC staff to receive presentations from cyber risk analytic vendors so that state insurance regulators can consider if the tools would be useful to them as regulatory tools.

### C. E-Commerce (H) Working Group

Director French said that the E-Commerce (H) Working Group has now exposed its state laws surveys/framework with comments due by March 23. The framework was developed based on survey work completed in 2022, which included questions on state laws, questions on actions taken in the wake of the COVID-19 pandemic, and a business impact survey.

Following the receipt of the comments, the Working Group plans to meet to further discuss the framework comments received and to consider the next steps required to meet the demands of the Working Group's 2023 charges.

## Draft Pending Adoption

### D. Innovation in Technology and Regulation (H) Working Group

Commissioner Conway said the Innovation in Technology and Regulation (H) Working Group plans to meet in April to develop a supotech regulator forum that would allow state insurance regulators to share insights on current innovations and technologies being explored among the regulatory community. The regulators will also look at developing an insurtech forum that would allow regulators to have confidential one-on-one discussions with insurers and third parties about innovation and technologies that insurers and third parties are using, as well as the regulations and barriers that may exist. The Working Group will also continue to monitor the developments of the Innovation, Cybersecurity, and Technology (ICT) Hub to ensure insights shared among the state insurance regulator community can be widely and easily distributed. The Working Group will continue to monitor industry trends, including consideration of training for regulators, which may lead to referrals to other working groups or committees.

### E. Privacy Protections (H) Working Group

Johnson said that on Feb. 1, the Privacy Protections (H) Working Group exposed a draft of the new *Insurance Consumer Privacy Protection Model Law* (#674) for a 60-day public comment period ending April 3. In the interim, the Working Group has met in regulator-to-regulator sessions on March 15 and Jan. 23. The Working Group met directly with companies on Feb. 16, March 1, 2, March 9, March 14, and March 19, with additional meetings scheduled for April 5, April 6, April 11, April 12, and April 13. The Working Group is also planning open meetings following the comment period beginning April 18 and an interim in-person meeting in Kansas City, MO, in June. The Working Group also met March 21 during the Spring National Meeting, during which it adopted its 2022 Fall National Meeting minutes, heard updates from Jennifer Neuerburg (NAIC) on state privacy legislation, heard updates from Shana Oppenheim (NAIC) on federal privacy legislation, and adopted its 2023 work plan. Commissioner Birrane commended the Working Group for its process thus far, noting that it has been rigorous and transparent.

Commissioner Godfreed made a motion, seconded by Deputy Superintendent Finston, to adopt the reports of the Big Data and Artificial Intelligence (H) Working Group (Attachment One), the Cybersecurity (H) Working Group (Attachment Two), the E-Commerce (H) Working Group, the Innovation in Technology and Regulation (H) Working Group, and the Privacy Protections (H) Working Group (Attachment Three). The motion passed unanimously.

### 3. Received an Update from the Collaboration Forum on Algorithmic Bias on the Development of a Model Bulletin Providing Regulatory Guidance Respecting the Use of Big Data/AI-Driven Decisional Systems by Insurers

Commissioner Birrane started the discussion by revisiting past discussions on the bulletin at the 2022 Fall National Meeting. Commissioner Birrane stated that bulletin work is a member-driven activity with a consensus that the framework developed should be principles-based and not prescriptive. The membership also has a consensus that the framework should focus on governance requirements and the establishment of protocols that rely on external and objective standards. The membership has also agreed that validations should be a part of the requirements but with recognition of the practical difficulties and limitations associated with testing. With respect to third parties, the preference among the membership was that responsibility be placed on licensees to conduct appropriate diligence with respect to third-party data and model vendors and to hold licensees responsible as opposed to attempting to directly regulate unlicensed third parties at this time.

Since the 2022 Fall National Meeting, state insurance regulators have started drafting the four sections of the bulletin among drafting groups. There is an introductory section with the leaders of that group: Director Popish Severinghaus, Commissioner Andrew R. Stolfi (OR), and Commissioner Nathan Houdek (WI). There is also a definitional section, of which the leaders are Commissioner Conway and Commissioner Gaffney. There is a section

## Draft Pending Adoption

focused on regulatory expectations, which is the largest section of the bulletin. This section's leaders are Commissioner Beard, Commissioner Birrane, Superintendent Dwyer, and Deputy Superintendent Finston. The final section of the bulletin is focused on regulatory oversight and examination based on the articulated standards. The leaders of that section are Commissioner Arnold, Commissioner Trinidad Navarro (DE), Commissioner Ommen, Commissioner Jon Pike (UT), and Director Wing-Heier.

Commissioner Birrane said she hopes to have a public exposure draft by the Summer National Meeting.

### 4. Heard a Report on the Colorado Proposed Algorithm and Predictive Model Governance Regulation

Commissioner Conway introduced Lapham, who provided an update on the Colorado proposed regulation. Lapham stated that the regulation under consideration is based on Senate Bill (S.B.) 21-169, which is designed to protect Colorado insurance consumers from insurance practices that result in unfair discrimination due to the use of predictive model AI tools. It applies broadly to insurers that use external consumer data and information sources (ECDIS), as well as the algorithms and predictive models that use ECDIS. The law requires that the Colorado Division of Insurance engages in stakeholder outreach for each type of insurance, with the Division initiating this process in February 2022. The Division has initially focused on life insurance underwriting and has held six stakeholder meetings thus far. Additionally, the Division completed a survey of 10 life insurers. In the process of stakeholder outreach, the Division has discovered that there is a wide range of insurer preparedness related to governance and risk management around AI tools. The Division bifurcated its approach to addressing the required risk management framework and testing components contemplated by S.B. 21-169 through two regulations.

The draft risk management framework regulation has three sections. The sections address governance framework expectations, documentation requirements, and a reporting requirement. The Division is in the process of digesting and synthesizing comments received and will adjust the regulations as appropriate with the intention of exposing a revised draft for additional comment. Commissioner Conway added that there has been an inaccurate view that once the Division notices the regulation, the discussion or opportunity for input is over. Commissioner Conway said this is not true. The Division continues to look forward to input regarding S.B. 21-169.

Birnbaum asked how many insurers will be submitting the annual reporting on their use of ECDIS, to which Lapham responded he does not have an answer apart from saying that as many carriers as are subject to the regulation. Commissioner Conway noted that the Division has not done a comprehensive survey of the companies to which the regulation will apply, so the Division is currently unable to provide an estimate apart from anticipating there will be a robust number of companies submitting the required information. Birnbaum followed up by saying that the reason for his inquiry is that, on the resources, the Division will need to review the insurance company reporting in a timely manner. Commissioner Conway said that is an issue that industry members have raised as well, and it will be one the Division is going to be cognizant of, as there is no point in requiring the testing or getting the required report if the Division cannot use it in a meaningful way.

### 5. Heard a Presentation on the Use of Block Chain Methodology for Data Calls

Commissioner Godfreed led a presentation on a North Dakota project to use blockchain technology for data calls. The reason for the data call initiative is to address several issues with data. The data available is often delayed, but the legislature meets on a biannual basis, with the data provided often being out of date. However, the North Dakota Insurance Department wants all policy decisions to be data-driven, noting that bad data can lead to bad public policy. Additionally, the data often available is usually higher in level than is needed to address the questions posed. The data-gathering process is often delayed as the Department tries to refine the questions being asked, which can lead to legislation not advancing or legislation advancing without the data needed. Data calls are often for a single point in time and are not easy to repeat. Lastly, Commissioner Godfreed noted that the data does not provide meaningful value to companies.

## Draft Pending Adoption

To address this problem, the Department undertook a pilot with one goal of the data call being to help answer the question regarding uninsured motorists, which is a frequent issue in every session of the legislature. The second goal was to test the data-gathering process/technology. Some industry estimates suggest the figure is as high as 20%, while others say it is as high as 7%, and the data available right now is likely 24 months old.

The Department gathered data by asking the North Dakota Department of Transportation (DOT) to provide the registers of vehicles in the state and relied on the 10 personal auto insurance companies with the most business in the state to provide data on the vehicles they insure in North Dakota.

Commissioner Godfread then described the mechanics of the technology, which, at a high level, can be explained as a highly secure, highly complex spreadsheet of information. The Department posted its list of vehicles registered in North Dakota. Carriers input their insured vehicle identification numbers (VINs) into a node created for each individual company. Information was then compared. No information ever left the nodes and thus stayed in the custody, control, and care of each company the entire time. This is different from a traditional data call, in which the data would have been copied and given to a third party or regulator, which raises a security issue consideration.

The Department ran into resistance, which required an extensive explanation of the technology and safeguards in place. However, once data was received, the Department found that among the 10 participating carriers, 46% of vehicles registered in North Dakota can be as insured in the top 10 auto carriers. The figure appears low, but Commissioner Godfread reminded the Committee that the data call only included 10 carriers and only focused on personal auto and that some companies provided information on recreational and farm auto VINs. Other vehicle types (e.g., motorcycles, classics, and recreational vehicles [RVs]) may also not be accounted for.

What the Department also found was that this data call was easy to repeat, with the first call going out on Feb. 10 and a repeat data call going out on March 10. The data call also allowed the Department to provide information back to carriers—for instance, that 21% of the VINs insured were not registered in the state. A final data call is expected on April 10. This data process could also be repeated to ask for more granular data as long as a data standard is set up, which sounds simple but has proved to be difficult. Still, because of the speed of the process and the information the process yielded, Commissioner Godfread considered the project a success.

Deputy Superintendent Finston asked if the Department ever took possession of the data. Aufenthie responded that the Department only received aggregated results based on the question posed. Godfread restated that the intent of the project was to prove that functionality was viable. Aufenthie noted that the American Association of Insurance Services (AAIS) created nodes for each individual company, and each company uploaded information into its node, but the nodes remained in their possession.

Commissioner Gaffney noted that this effort is very timely, as states are in legislative session, so this technology may be beneficial from an efficiency and data security standard. Commissioner Gaffney asked what expertise would be needed to complete the project or if the expertise was provided by the vendor. Commissioner Godfread remarked that the resources/costs were not substantial but that the key hurdle was generating willingness to embark on the project as it required many discussions with stakeholders, especially if departments of insurance (DOIs) continue with parallel data tracking mechanisms while the blockchain technology continues to be validated for data call usage. Commissioner Godfread noted that smaller companies did find the project beneficial in that they were able to access meaningful data that was gathered as part of the project. Commissioner Godfread further noted that while there may be a cost associated with the technology, it is negligible compared to the cost associated with the current data-gathering processes.

## Draft Pending Adoption

Darby, Statistical Data (C) Working Group chair, noted that the Working Group had been looking at blockchain technology/OpenIDL technology for a similar project and asked if there was a cost figure per company or if figures were able to compare costs between smaller and larger companies. Aufenthie noted that there was zero cost to the companies participating in the process. However, he said that he was unsure about cost to the vendor and expects the cost would go down as an increasing number of companies participate in the process. Darby also asked about the security of the data in the node. Aufenthie noted that the program was permission-based, which helped avoid security issues. The companies were able to see and understand the information that would be shared, which required some upfront discussion about the technology, but the fact that the information stays with the company the entire time means it is more secure than the current process. Under the current process for data calls, data is transmitted to a third party, which is less secure. Additionally, DOIs are able to limit access to the data to only the data fields that are truly needed for the information-gathering exercise.

Bradner noted that in their own experience with OpenIDL, the initial setup can be time-consuming, but it can be easily repeated once set up. Bradner hopes that state insurance regulators can continue to build data-gathering capabilities leveraging OpenIDL technology.

Hirano asked how, if the Department did not ever have the data locally, it was able to determine that farm and recreational vehicles were included in the data set. Commissioner Godfread noted that as companies were uploading information, they informed the Department about what was being uploaded. Therefore, this determination did not come out through the blockchain analysis phase of the project but instead was identified in the early discussions before data was uploaded.

Commissioner Birrane asked how long the project took to get started. Aufenthie stated that the project started in June 2022 with the hopes of getting done by the end of the year, but the project took a long time to get started, specifically with getting companies comfortable with the technology. The Department started the discussions with a day-long summit to talk about the technology and intent of the project, which was beneficial, but the companies still raised many questions as the project moved along.

Commissioner Birrane asked what the North Dakota Insurance Department sees as the challenge going forward. Commissioner Godfread said that a data standard is the largest obstacle. Working with VINs was manageable, but as the complexity of the data call increases, so will the complexity of the data standards. Therefore, asking for very specific information may prove to be difficult.

Birnbaum thanked North Dakota for its willingness to engage in the data call pilot project. Birnbaum asked about resource requirements for the DOIs to continue with the data calls. Aufenthie said the resource requirements are minimal because most of the work of the project comes in the setup. Asking for a data refresh, as anticipated in April, will take one minute to complete. Aufenthie noted that this project resulted in no additional staffing needs and no cost to the state. Birnbaum then asked how difficult it would be to expand the data call project to include zip codes and then produce the same uninsured data by zip code. Aufenthie said it would not be difficult to expand the data call as such but would require upfront work with the vendor to ensure the coding is updated. Aufenthie noted, however, that adding ZIP codes could introduce privacy issues that would need to be considered.

Tony Cotto (National Association of Mutual Insurance Companies—NAMIC), thanked North Dakota for the process undertaken, including involving the trades, as it helped build comfort with the project. Cotto also noted that while answering the uninsured motorist problem was not the true intent of the data call, it is still an important issue for states to consider. Cotto noted that the Insurance Industry Committee on Motor Vehicle Administration (IICMVA) is also looking at blockchain technology, specifically regarding motor vehicle authentication.

## **Draft Pending Adoption**

Robin Wescott (AAIS) thanked Aufenthie for his work on the project and noted that cost is difficult to determine, even for the current data-gathering process, but noted that the blockchain project might yield efficiencies. Wescott also noted that the technology this was built upon is the hyper ledger fabric through the Linux Foundation, which is an open software solution. Wescott encouraged the industry to look at open-source solutions, not just proprietary ones. This technology could affect the statistical reporting process, perhaps even removing the need for statistical agents. Wescott said the AAIS supports this because its goal is to make data easier to access.

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

SharePoint/NAIC Support Staff Hub/Member Meetings/H Cmte/2023\_Spring/H-Cmte Minutes032223-Final.docx



## Draft Pending Adoption

Draft: 4/4/23

Big Data and Artificial Intelligence (H) Working Group  
Louisville, Kentucky  
March 22, 2023

The Big Data and Artificial Intelligence (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Louisville, KY, March 22, 2023. The following Working Group members participated: Elizabeth Kelleher Dwyer, Chair (RI); Amy L. Beard, Co-Vice Chair, represented by Victoria Hastings (IN); Doug Ommen, Co-Vice Chair (IA); Kevin Gaffney, Co-Vice Chair (VT); Sarah Bailey (AK); Mark Fowler (AL); Peg Brown and Jason Lapham (CO); George Bradner and Wanchin Chou (CT); Michelle Brewer (FL); Shannon Hohl (ID); Erica Weyhenmeyer (IL); Abigail Gall (KY); Tom Travis (LA); Jackie Horigan (MA); Kory Boone (MD); Timothy N. Schott and Sandra Darby (ME); Karen Dennis (MI); Grace Arnold (MN); Cynthia Amann (MO); Robert Croom (NC); Chris Aufenthie, John Arnold, and Colton Schulz (ND); Connie Van Slyke and Martin Swanson (NE); Christian Citarella (NH); TK Keen (OR); Shannen Logue (PA); Ryan Basnett (SC); Travis Jordan (SD); Stephanie Cope (TN); Leah Gillum (TX); Tanji J. Northrup (UT); Eric Lowe and Katie Johnson (VA); Molly Nollette (WA); Nathan Houdek and Lauren Van Buren (WI); and Erin K. Hunter (WV). Also participating were: John F. King (GA); Troy Downing (MT); and Matt Gendron (RI).

### 1. Adopted its 2022 Fall National Meeting Minutes

Commissioner Gaffney made a motion, seconded by Cope, to adopt the Working Group's Dec. 13, 2022, minutes (see *NAIC Proceedings – Fall 2022, Innovation, Cybersecurity, and Technology (H) Committee, Attachment Two*). The motion passed unanimously.

### 2. Received an Update on the AI/ML Surveys

Commissioner Gaffney said the purpose of the home survey is to gain a better understanding of the industry's use of big data, artificial intelligence (AI), and machine learning (ML), as well as what governance, risk management, and controls are being put in place in developing and managing those activities. The survey also seeks to gather information that may inform the development of guidance or a potential regulatory framework that would support the insurance industry's use of big data and AI/ML in accordance with the expectations outlined in the NAIC's AI Principles. As previously reported to the Working Group, the formal examination call letter was sent to 194 companies. Any company licensed to write home insurance in one of the 10 Requesting States that also had at least \$50 million in national home insurance premiums for 2020 was required to complete the survey.

Commissioner Gaffney said survey responses were due by Dec. 15, 2022. The Requesting States were still awaiting responses from eight companies as of March 1. A final request was sent to these companies on March 3 with a response deadline of March 24. Once the survey is closed on March 24, NAIC staff will begin working with the Requesting States to produce a public report, similar to the Private Passenger Auto (PPA) Report. As with the PPA Report, the confidentiality of individual company responses will be protected. The Requesting States will present a public report to the Working Group at the Summer National Meeting.

Commissioner Gaffney said a group of 14 states continued to develop the life insurance survey with the goal of collecting information to understand how life insurance companies are deploying AI/ML in the following operational areas: 1) pricing and underwriting; 2) marketing; and 3) loss prevention. Like the PPA survey and the

## Draft Pending Adoption

home survey, the goal of the life insurance survey is to learn directly from the industry about what is happening in this space to get a sense of the current level of risk and exposure associated with their use of AI/ML and how the industry is managing or mitigating that risk. The following criteria were used to identify which companies should receive the survey: 1) a company with more than \$250 million in premiums on all individual policies in 2021; 2) a term writer that has issued policies on more than 10,000 lives; or 3) a specifically selected InsurTech company. Using these criteria, the 14 Requesting States, which will collect the survey information under their examination authority, will issue a formal examination call letter to a total of 192 life insurance companies.

An informational letter should be sent to the 192 companies on March 31. Coinciding with the issuance of this letter, the NAIC will go live with the AI/ML life insurance survey weblink, which will include the survey template, survey filing guidance and definitions, and a frequently asked questions (FAQ) document. Concurrently, each company will receive a survey link and can begin to input their answers into the Qualtrics survey tool even before the official call letter is sent. Commissioner Gaffney said each company scheduled to receive the survey should have designated one contact to receive the survey link, and they can forward it to anyone in their company who has the information needed for the survey. The tool allows multiple people in a company to input answers and saves the most up-to-date information input into the survey.

Commissioner Gaffney said the formal examination call letter is scheduled to be issued on May 1, and companies will have until May 31 to respond to the survey. The Requesting States hope this timeline will help accommodate those companies also filing Market Conduct Annual Statement (MCAS) data due April 30.

Superintendent Dwyer reminded everyone that the PPA public report is posted on the Working Group's web page, and she is not aware of any comments on or concerns about this report.

### 3. Discussed Draft Model and Data Regulatory Questions

Commissioner Ommen said the subject matter experts (SMEs) assembled for Workstream #2 were asked last year by the Working Group to provide recommendations for: 1) the feasibility of a library of third-party data and model vendors with AI-known applications in the business of insurance; and 2) an appropriate regulatory framework for monitoring and overseeing the industry's use of third-party data and model vendors. In accordance with the second charge of the Working Group, the state insurance regulators on Workstream #2 exposed for discussion draft questions that state insurance regulators might ask about data and models used by insurance companies, regardless of whether the data or model is developed internally or obtained from external sources. These questions were meant to be a starting point for discussion, and there needs to be further work.

Commissioner Ommen provided a summary of the document. The first section, titled "Main General Questions," includes a list of suggested questions to obtain a high-level understanding of a model or data being used. The second section, titled "Detailed and Technical Questions," expands on the first section by including additional questions to obtain a more in-depth understanding of the model or data. The questions are subdivided into three categories within each of these first two sections. The first category contains questions to ask a company about a model, whether the company is an insurer or a third party. The second category contains questions to ask an insurer about its implementation of a third-party model. The third category contains questions about the purchase of third-party data. Finally, the third section in the document contains definitions of key terms used throughout the document. Commissioner Ommen said he is not satisfied with the definitions, which are meant as "placeholder" definitions.

## Draft Pending Adoption

Commissioner Ommen said the SMEs of Workstream #2 had a call on March 8 and began discussing the following policy issues raised in the comment letters: 1) the document should be principle-based; 2) the document should be more limited in scope to encourage state insurance regulator use for “higher-risk” AI models; 3) questions should be prioritized to recognize the importance of model governance; 4) there are concerns that questions contain assumptions of law that are not based in law; 5) there are concerns regarding redundancy with financial examinations; 6) there are concerns with the potential burden on smaller companies and small AI providers; and 7) clarification of the intended use of questions by state insurance regulators is needed. He said a smaller group of the Workstream SMEs will review the comments and hope to present a revised draft for public comment by the end of May.

Birny Birnbaum (Center for Economic Justice—CEJ) said insurers use data models through the insurance life cycle, including marketing, underwriting, pricing, antifraud, and claim settlements. He said state insurance regulators have a responsibility to ensure that rates are not excessive, inadequate, or unfairly discriminatory, and he said the document should identify regulatory authorities and responsibilities. He said state insurance regulators can best fulfill their responsibilities by analyzing the outcomes of data models rather than asking questions to understand how an insurer developed a data model. He said state insurance regulators do not have the resources to review and analyze insurers’ narrative responses, and state insurance regulators should collect additional data from insurers to ensure that model outcomes comply with state laws rather than focusing on an insurer’s process of model development.

David Leifer (American Council of Life Insurers—ACLI) said the scope of information to be collected is overly broad, especially regarding third-party vendors and the ability of insurers to produce proprietary information from third-party vendors. David F. Snyder (American Property Casualty Insurance Association—APCIA) also said the questions should be grounded in existing state laws. He said the definitions need to be revised. He also encouraged additional coordination of this work with other workstreams across the NAIC, such as the Accelerated Underwriting (A) Working Group and the Innovation, Cybersecurity, and Technology (H) Committee’s work on the AI model bulletin.

Andrew Pauley (National Association of Mutual Insurance Companies—NAMIC) said NAMIC has concerns with the questions not being based on state regulatory requirements. He said the definitions need to be revised, and he encouraged this work to be coordinated with other NAIC workstreams. He suggested that the state insurance regulators focus on a principle-based approach, and he questioned why all information would be requested at once. He also expressed concern regarding the protection of confidential proprietary information that might be provided.

Scott Harrison (American InsurTech Council—AITC) suggested a risk-based approach, and he voiced concern that the scope of questions would create a disproportionate burden on smaller companies. He suggested that state insurance regulators should focus on only those AI models that affect consumers or a company’s financial solvency since companies use models that do not have regulatory implications. He also expressed concerns regarding the protection of confidential information, especially the protection of proprietary information.

Snyder said the creation of a uniform set of questions is helpful, but the scope and detail of the questions are very broad. He said there are concerns with the definitions, and he suggested that state insurance regulators should consider the risk, scale, and complexity of a company when asking about its AI models. He urged that testing not be included in the document due to the complicated nature of AI model testing. He said it is not clear what

### **Draft Pending Adoption**

standard is being tested and how much is too much of a relationship to a protected class. Snyder also said confidentiality protections are important, and the disclosure of propriety models of third-party vendors can be very complicated. Finally, Snyder encouraged everyone to remember that the use of AI models makes it possible for the industry to provide better services to consumers.

Bob Ridgeway (America's Health Insurance Plans—AHIP) said any use of these questions should be under examination authority to protect the confidentiality of responses. He said insurers are familiar with submitting confidential information to state insurance regulators, but third-party vendors are not comfortable with sharing proprietary information. He said third-party vendors might not have any appropriate recourse if a governmental agency is the source of propriety information being shared with the public. He said the scope of the questions would require insurers to share a voluminous amount of information, and he suggested that higher-level information be collected first. This would make it easier for companies to respond and for state insurance regulators to review the information.

Peter Kochenburger (University of Connecticut School of Law) said state insurance regulators should not look at these issues only through the application of existing state laws. State insurance regulators should be setting expectations, and if needed, they can amend existing laws and regulations to address the use of AI in the insurance industry.

Superintendent Dwyer said the Innovation, Cybersecurity, and Technology (H) Committee is coordinating the AI work across the NAIC, including the activities of Workstreams #3 and #4. Workstream #3 is charged with evaluating tools and resources for monitoring the industry's use of data and AI/ML, and Workstream #4 is focusing on the broader regulatory framework and governance.

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

SharePoint/NAIC Support Staff Hub/Member Meetings/H Cmte/2023\_Spring/WG-BDAI/BDAI-Minutes032223-Final.docx

Draft: 4/6/23

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

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

1. Adopted its 2022 Fall National Meeting Minutes

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

2. Discussed its Work Plan for 2023

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. Discussed the Outline for the Incident Response Plan

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

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

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

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

6. Discussed Other Matters

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

SharePoint/NAIC Support Staff Hub/Member Meetings/H CMTE/2023\_Spring/WG-Cybersecurity/Cyber-WG-Minutes030723.docx



## The Cybersecurity (H) Working Group 2023 Workplan:

### Working Group Charges:

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

- 
- Workstream 1: Cybersecurity Response Plan

Subject Matter Expert Group Lead: Cindy Amann/Michael Peterson

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

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

Timeline: Completed by 2023

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

Considerations: Regulators should consider:

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

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

Subject Matter Expert Group Lead: N/A

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

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

Related Charges: This project would fall under charge E.

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

---

- Workstream 3: Training

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

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

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

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

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

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

---

- Workstream 4: Monitoring

Subject Matter Expert Group Lead: Wendy Erdly

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

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

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

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

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

SharePoint/NAIC Support Staff Hub/Member Meetings/H CMTE/2023\_Spring/WG-Cybersecurity/work plan 2023.docx



---

**MEMORANDUM**

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

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

DATE: March 7, 2023

RE: Cybersecurity Procedures

---

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

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

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

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

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

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

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

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

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

SharePoint/NAIC Support Staff Hub/Member Meetings/H CMTE/2023\_Spring/WG-Cybersecurity/Referral to IT Examination WG.docx

## Draft Pending Adoption

Draft: 4/11/23

Privacy Protections (H) Working Group  
Louisville, Kentucky  
March 21, 2023

The Privacy Protections (H) Working Group of the Innovation, Technology, and Cybersecurity (H) Committee met March 21, 2023. The following Working Group members participated: Katie Johnson, Chair (VA); Cynthia Amann, Co-Vice Chair (MO); Chris Aufenthie, Co-Vice Chair (ND); Catherine O’Neil (AZ); LeAnn Crow (KS); Kathleen A. Birrane and Alexander Borkowski (MD); Robert Wake (ME); T.J. Patton (MN); Troy Downing (MT); Martin Swanson (NE); Michael Humphreys and Gary Jones (PA); Patricia Smock (RI); Frank Marnell (SD); Amy Garcia (TX); Mike Kreidler and Todd Dixon (WA); and Rachel Cissne Carabell, Timothy Cornelius, and Lauren Van Buren (WI). Also participating were Peg Brown (CO); John F. King (GA); Doug Ommen (IA); Victoria Hastings (IN); Jo LeDuc (MO); John Arnold (ND); Travis Jordan (SD); and Don Beatty (VA).

### 1. Adopted its 2022 Fall National Meeting Minutes

Johnson said the Working Group met Dec. 12, 2022. The Working Group also met March 15, 2023, and Feb. 16, 2023, in regulator-to-regulator session, pursuant to paragraph 8 (consideration of strategic planning issues) of the NAIC Policy Statement on Open Meetings, to discuss its next steps.

Amann made a motion, seconded by Aufenthie, to adopt the Working Group’s Dec. 12, 2022, minutes (*see NAIC Proceedings – Fall 2022, Innovation, Technology, and Cybersecurity (H) Committee, Attachment Five*). The motion passed unanimously.

### 2. Heard an Update on Federal and State Privacy Legislation

Jennifer Neuerburg (NAIC) said that there had been a lot of activity since the 2022 Fall National Meeting, but she was going to try to keep her update brief because she knew a lot of people were waiting to comment on the exposure draft. Neuerburg said there are currently around 50 bills under consideration across 21 states.

She said the Iowa legislature passed a consumer data privacy bill on March 15 that is similar to Utah’s privacy law and business friendly. While the bill is pending the governor’s signature, she said Iowa would become the sixth state to pass a comprehensive data privacy bill. Neuerburg said Hawaii and Indiana are considering bills that are similar to the Virginia Consumer Data Protection Act. She said there are also bills being considered in New Jersey, Montana, and Oklahoma, just to name a few other states.

Neuerburg said charts tracking the legislation will be posted on the Privacy Protections (H) Working Group’s web page if anyone wants to read more about these bills. She said the NAIC’s legal team will continue to follow state data privacy legislation and provide updates at future Working Group meetings.

Shana Oppenheim (NAIC) said there had been a lot of activity on the federal side. In the House Financial Services Committee, she said Chair Patrick McHenry’s (R-NC) financial data privacy bill, the Data Privacy Act of 2023 (H.R. 165) has passed out of committee along party lines. Oppenheim said it would revamp existing data privacy protections for consumers by providing a preemptive ceiling and floor in an attempt to create a uniform federal standard. For enforcement by the functional regulators, the current bill provides a new deletion right for

## Draft Pending Adoption

consumers and allows consumers to stop the collection and disclosure of their data, among other provisions. She said U.S. Rep. Maxine Waters (D-CA) and other Democrats have been critical of the exemption because it would hinder a state's ability to: "Act as a laboratory for innovation while establishing what they see to be a weak federal standard."

Oppenheim said the House Committee on Energy and Commerce has an Innovation, Data, and Commerce Subcommittee that also recently held a hearing like a hearing for a federal national standard on data privacy. She said this follows up on the work from the last Congress, when the House Committee on Energy and Commerce leaders and then senior commerce ranking member, U.S. Sen. Roger Wicker (R-MS), compromised on the American Data Privacy Protection Act (H.R. 8152). Oppenheim said Chairwoman Maria Cantwell (D-WA) did not sign. The bill still passed the House Committee on Energy and Commerce and was being considered for the Omnibus bill, but it was ultimately not included. She said this preemptive bill would create a national standard and safeguards for personal information collected by companies, including protections intended to address potentially discriminatory impacts of algorithms. Oppenheim said the bill is expected to be reintroduced in some form, so federal action is expected to be ongoing.

### 3. Considered its Updated 2023 Work Plan

Johnson gave an overview of the Working Group's updated work plan, dated March 13. She said the workplan is posted on the Working Group's web page and indicates that the exposure draft of the new model was distributed on Feb. 1 for a two-month public comment period ending April 3. Johnson said the revised work plan extends the date by which the model will be sent to the Innovation, Cybersecurity, and Technology (H) Committee to the Fall National Meeting. She said the Working Group did that because it had received so many comments from interested parties, and it wanted to give everyone enough time to consider those comments.

Johnson said the revised work plan lists April 18 as the date that biweekly Working Group meetings will resume to discuss comments received in open meetings. She asked that all parties come prepared to roll up their sleeves and get to work on refining the wording in the draft exposure model.

Johnson said a two-day, in-person, interim Working Group meeting is also being planned for June in Kansas City, MO, to work through the more complex issues identified in the model using transparent collaborations to address those issues in a way that makes the model workable for state insurance regulators, those in the industry, and consumers. She said many of the more complex issues have already been identified by the drafting group in private meetings with volunteer companies. Johnson thanked the companies that had stepped forward to discuss these complex issues. She said many of the industry trade associations and consumer representatives were included in those who volunteered. She said the Working Group was grateful for their help.

### 4. Received and Discussed Comments on the Exposure Draft of the New Model #674

Johnson said the Working Group would hear preliminary comments from interested parties on the exposure draft of the new *Consumer Privacy Protection Model Law* (#674) in advance of the 60-day public comment period ending April 3.

Harry Ting (Healthcare Consumer Advocate) said he was also a Senior Health Insurance Information Program (SHIIP) counselor who has counseled more than 400 people who qualify for Medicare and Medicaid. He said the comments he submitted in more detail in writing on the new draft of Model #674 expressed his strong support

### **Draft Pending Adoption**

for it and suggested a few changes. Dr. Ting said since getting involved in this Working Group, he has become more aware of how personal information is captured and misused. He said whenever he goes to a new website now, he tries to minimize the data that can be stored and used. He also tries to read the entire privacy policy to understand how to exercise that option. However, he said sometimes it takes too much time, and sometimes, he is given no choice if he wants to use the site. Dr. Ting said he experiences abuse of his personal data daily. He has had his credit card information stolen and gets so many unwanted marketing emails that the emails he wants to see get lost in a sea of unwanted emails. Dr. Ting said the worst of it is that it seems to be occurring more frequently. He said he gets phishing emails and texts disguised as urgent messages from companies he uses trying to steal his personal information. In addition to that, he cannot escape losing his information, as it is being shared by his phone, TV, car, and appliances through the Internet of Things (IoT) in this environment. He said he wishes the federal government would do more to protect his personal information, but that it is unlikely because Google and Meta base their business upon it.

Dr. Ting said now is the time for state insurance regulators to pass fair consumer data privacy legislation for the insurance industry because the key players in this realm are not taking any action. He said he was pleased to see that the draft of Model #674 establishes clear standards for protecting consumer privacy in the areas of: 1) transparency and data minimization; 2) use limitations by review and correction; and 3) requiring third-party service providers to meet the same privacy and accountability standards as licensees. Recognizing that not all states and territories will adopt this model, he said he hopes that many insurance companies and licensees will adopt these privacy protections anyway. By doing so, Dr. Ting said companies are likely to meet the requirements of the states where they do business. He said there are six reasons why consumer data privacy standards are needed and three revisions that he recommends. He said claims that standards are not needed because consumers are not complaining are invalid because consumers have no way of knowing that their data is being used or how it is being shared with others for their use. Dr. Ting said privacy protections must be the default of privacy protection policies should always be the default of non-disclosure. He said it is well documented that most consumers do not read entire privacy policies and that it is not realistic to expect them to do so nor to expect them to understand what is in them because privacy policies are notoriously long and complex. Moreover, Dr. Ting said companies use dark patterns that manipulate consumers into permitting greater use of their data than the consumer had intended.

Dr. Ting said that Health Insurance Portability and Accountability Act of 1996 (HIPAA) standards should apply to all personal information. Dr. Ting said when HIPAA was enacted, it stated that personal health information was more sensitive and needed more protection than personal financial information. However, time has proven that to be false, as personal financial information has been used fraudulently to significantly harm millions of Americans. He said the same standards should apply to third-party service providers as to insurance providers and licensees because the risk of abuse of personal information is the same for both groups. Dr. Ting said because most states do not have regulatory authority over third-party service providers, it is even more important that the model includes these providers in its privacy protection standards through their contracts with insurance carriers that are regulated by state insurance departments. He said data minimization is essential because it is impossible to totally prevent data breaches and that over the past five years, insurance companies as diverse as Prudential Financial, John Hancock, Allstate, and State Farm have each reported multiple data breaches. He said major third-party providers have also reported breaches by Blue Cross Blue Shield Association (BCBSA), a medical imaging group, a professional health care collection agency, and Verisk Analytics—one of the world's largest data aggregators.



## Draft Pending Adoption

Dr. Ting said last month in Congress, the Electronic Privacy Information Center (EPIC) agreed that all companies should limit their data collection to only what is reasonably necessary and appropriate to provide or maintain a product or service requested by an individual. He said that is exactly what is illustrated in the draft of Model #674 and that compliance with it is the key. Dr. Ting said Model #674 will only be effective if it has meaningful penalties for serious noncompliance because there is no practical way for state insurance regulators to adequately monitor thousands of licensees and third-party service providers. He said there are three specific recommendations:

- Article 3, Section 7, should also require disclosure of consumer reporting agencies used and to the extent they use their third-party services to obtain and share consumers' personal information.
- Article 5, Section 14, should be revised, and it should not be optional because consumers should have the ability to obtain detailed reasons for insurance companies' adverse underwriting decisions immediately and not be required to provide a written request to the company to get those details.
- Data security and privacy are inextricably connected, so data security requirements such as those in the *Insurance Data Security Model Law* (#668) need to be added to this model so third-party service providers and licensees that have access to consumer data are held to the same standards as the insurance companies they contract with.

Johnson said a joint trade group also submitted comments in advance of the comment deadline, which are included in the materials posted on the webpage for this meeting. She asked if anyone would like to provide comments on the draft model.

Kristin Abbott (American Council of Life Insurers—ACLI) said companies and people need standards for privacy protections but do not need an overly prescriptive model. To avoid friction and unnecessary new barriers, she said the key is prior consent for marketing because requiring it would hurt underserved markets, prohibit joint marketing, increase costs and premiums, harm small to mid-sized companies, restrict research, and limit actuarial services. Abbott said overseas processing is difficult to track, and putting privacy restrictions on them would harm international insurers. It would also result in decreased services for customers, which is why the General Data Privacy Regulation (GDPR) does not even require this. She said the 90-day deletion requirement needs to be removed from the model, as most companies with legacy systems will not be able to accommodate this standard. Abbott said the new notice and oversight requirements in the model would increase implementation costs because insurers use personal information to provide products to meet their needs.

Robert Ridgeway (Americas Health Insurance Plans—AHIP) said he was speaking on behalf of both HIPAA-compliant and non-HIPAA-compliant companies. He said the companies he represents like the new timetable and the schedule of future meetings, including the interim, in-person meeting being planned. Ridgeway said the Working Group's plan to handle low-hanging fruit in the form of less complex privacy issues during meetings would be productive. He said the partial exemption for HIPAA issues should be made a complete exemption via safe harbor for HIPAA-compliant companies. Ridgeway said the operative sections should be what companies need to do or not do and should not pertain to activities that are already covered by HIPAA so that companies are not trying to wade through duplicate obligations. He said for other non-HIPAA-compliant companies, the pinch points are: 1) private right of action where verbiage the same as Model #668 would be a good choice; and 2) whether the sharing of personal data overseas should be considered a privacy or cybersecurity issue.

Aufenthie asked that written comments be submitted describing where in the model the partial safe harbor for HIPAA (Sections 2, 9, 10, 11, 12, or 13) should be changed to a full safe harbor incorporating oversight of third-party contracts, including business associates and how they think it should be worded.

### Draft Pending Adoption

Shelby Schoensee (American Property Casualty Insurance Association—APCIA) said that several members have met with the drafting group. They want an in-person interim meeting, will be submitting written comments, and will be actively engaged in the collaboration process. She said their primary concerns are: 1) the overseas data privacy requirement because many of the companies operate on a global basis that relies on the data market; 2) the marketing and research limitations, as they would prevent joint marketing; 3) third party oversight, which is a contractual issue, so a delayed effective date (like the risk-based approach in Model #668) for implementation is imperative; 4) the private right of action; 5) the new notice requirements; and 6) the inconsistent language about actuarial studies. Schoensee said the Working Group needs to find an appropriate balance between a consumer's needs and a company's right to market its products.

Birny Birnbaum (Center for Economic Justice—CEJ) asked what an appropriate balance between consumer needs and company marketing would be.

Commissioner Humphreys said this question came up with the ACLI, AHIP, and now the CEJ. Ridgeway took a little different tact with the unsolicited sales and marketing by saying state insurance regulators do not want to curtail a company's ability to do that, whereas Schoensee and Ridgeway both mentioned wanting to protect policyholders' money and not wasting it. He said he was trying to figure out what the balance was because he would argue that a lot of the unsolicited sales that he gets today are a waste. Commissioner Humphreys said there is a bit of a challenge here. He equated this to a non-insurance example of closing on a house and then getting 73 calls about the mortgage rate for the next two days—all unsolicited and all unwanted—blocking his phone. So, then, where do we draw the line if we are concerned about the policyholders' money but also want you to be able to continue to make these offers? Schoensee said that finding the balance is one of the issues that need to be addressed in the in-person meeting.

Wes Bissett (Independent Insurance Agents and Brokers Association—IIABA) said he was surprised by the draft because the changes to it were so extensive and that the Working Group had gone too far in restricting companies' and producers' use of consumer data. He said it should be much broader to allow licensees to operate efficiently.

Aufenthie suggested that the IIABA submit detailed written comments with specific reasons why existing wording would not be effective and suggest new wording that would address the pain points noted rather than giving broad disapproval of the draft model out of pocket without providing constructive criticism or solutions.

Chris Peterson (Coalition of Health Insurers) said HIPAA preemption changes to the proposed privacy rule should be reworded to read, "if companies comply with" rather than "is subject to," and that it should be a safe harbor for those companies deemed to be HIPAA-compliant rather than an exemption. He said other sections brought under the safe harbor would be business associate agreements for third-party businesses because health care providers expect to see it in order to keep a lack of confusion, as he said HIPAA is more robust than the draft model in all areas. Aufenthie suggested that health care providers go through each of the sections in the model, indicating where in HIPAA the sections could be found that indicated more robust consumer data privacy than that in the draft model. Peterson said the offshore data issue is a federal constitutional issue and that there should be no private right of action due to federal labor issues.

Cate Paulino (National Association of Mutual Insurance Companies—NAMIC) said that the opt-in requirement was a showstopper, especially when it came to sharing data outside of the U.S., as companies would lose their efficiencies by providing servicing for consumers 24/7. She said the annual notice requirement violated the federal Fixing America's Surface Transportation (FAST) Act, which eliminated the need to send annual notices and has

### **Draft Pending Adoption**

been enacted in 47 states. Paulino said the model should use categories of sources for data minimization, not be so prescriptive, and not limit the application process because hundreds of thousands of licensees would be subject to contract issues. She said that exemptions were necessary as are delayed effective dates to comply. Paulino said that exclusivity as to insurance versus general business practices should be implemented and that there should be no private right of action.

Jeffrey Klein (McIntyre & Lemon) asked that the Working Group reconsider the wording of Article 4, Section 4, and said that he would submit detailed suggestions as to the changes along with his clients' reasons for requesting such changes. Wake said the deletion of marketing was intentional due to the cause versus benefit analysis. Peter Kochenburger (Southern University of Law—SULC) said it was this issue that caused Wells Fargo to be forced to sell its insurance business and financial products in order to prevent massive fraud. Johnson said this issue would be one of the more complex issues that would be addressed at the in-person interim meeting.

#### **5. Discussed Other Matters**

Johnson reminded attendees about the Working Group's two-day, in-person interim meeting tentatively scheduled for June 4–6 in Kansas City, MO.

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

SharePoint/NAIC Support Staff Hub/Committees/H Committee/2023\_Spring/Minutes\_National Meeting\_PPWG\_Final