INNOVATION, CYBERSECURITY, AND TECHNOLOGY (H) COMMITTEE

Draft Pending Adoption

Draft: 8/28/24

Innovation, Cybersecurity, and Technology (H) Committee
Chicago, Illinois
August 15, 2024

The Innovation, Cybersecurity, and Technology (H) Committee met in Chicago, IL, Aug. 15, 2024. The following Committee members participated: Kevin Gaffney, Chair (VT); Michael Conway, Co-Vice Chair, represented by Kate Harris (CO); Chlora Lindley-Myers, Co-Vice Chair, and Cynthia Amann (MO); Ricardo Lara (CA); Karima M. Woods and Sharon Shipp (DC); Michael Yaworsky and Alexis Bakofsky (FL); Gordon I. Ito (HI); Doug Ommen (IA); Ann Gillespie and KC Stralka (IL); Joy Y. Hatchette and Kory Boone (MD); Troy Downing (MT); Jon Godfread represented by Colton Schulz (ND); Judith L. French represented by Matt Walsh (OH); Michael Humphreys (PA); and Alexander S. Adams Vega represented by Iris M. Calvente Galindez (PR). Also participating were: Lori K. Wing-Heier (AK); Weston Trexler (ID); Amy L. Beard (IN); Tom Travis (LA); Christian Citarella (NH); Elizabeth Kelleher Dwyer and Matt Gendron (RI); Cassie Brown (TX); Jon Pike (UT); and Scott A. White (VA).

1. Adopted its June 28 Minutes

The Committee met June 28 and took the following action: 1) adopted its Spring National Meeting minutes; 2) received an update on its workstreams; and 3) heard presentations from consumer representatives on consumer protection proposals and privacy protections.

Commissioner Gaffney noted a modification to the June 28 minutes, adding Anoush Brangaccio (FL) to the participant list.

Commissioner Lara made a motion, seconded by Commissioner Ommen, to adopt the Committee's June 28 minutes (Attachment One). The motion passed unanimously.

2. Adopted its Task Force and Working Group Reports

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

Bakofsky reported that the Task Force was established this year to address the growing concerns among commissioners regarding the use of third-party data and models to ensure that state insurance regulators can confidently assure consumers, stakeholders, and state governors of the fair use of data and models by insurers.

The Task Force's initial action was the formulation and adoption of a 2024–2025 work plan, which is bifurcated into two distinct phases. The first phase involves a thorough research step to evaluate existing regulatory frameworks, assess their applicability to regulating third-party data and models, and establish objectives for a future regulatory framework. Upon completing this phase, the second phase will focus on constructing the third-party regulatory framework. The Task Force is committed to conducting meticulous research and maintaining an open and transparent process to ensure well-informed and judicious decision-making.

On July 30, the Task Force heard presentations about national and state-centric U.S. risk-based regulatory approaches and presentations to provide insights into regulatory decision-making and the role of experts in assisting state insurance regulators. The Task Force is taking a blended approach that is national and market-wide in terms of the framework but flexible such that a state can focus on the risks and models applicable in that state. The next steps include engaging with the European Union (EU) to gain insights into Solvency II's risk-based approach and identifying and inviting speakers to inform the Task Force about relevant frameworks outside of insurance regulation that could be beneficial in this context.

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

Commissioner Humphreys reported that the Working Group met July 29. The Working Group received an update on the health artificial intelligence (AI)/machine learning (ML) survey work, including piloting the survey with a few selected companies. The survey is intended to go live later this year, with plans to post the survey publicly no later than early October. The survey includes questions tailored to the use of AI in the operational functions of health insurers related to data usage, arrangements with third parties, and coordination with existing health provider governance standards. A selected group of companies that have completed the auto surveys have been targeted for follow-up regulator-only discussions to ask whether they have begun to use or have changed their use of AI/ML in their operations, including generative AI, since the auto survey was completed in 2021.

During that meeting, the Working Group also received a presentation from Dorothy Andrews (NAIC) on the Society of Actuary's (SOA's) research on inference methods, which covered several topics, including the Bayesian Improved First Name and Surname Geocoding (BIFSG) method and examples of results from using this method. The Working Group also discussed the underlying data used by the BIFSG method, its limitations, and concerns about accuracy.

C. Cybersecurity (H) Working Group

Amann reported that the Working Group met Aug. 14 and took the following action: 1) adopted its July 9 minutes, which included the following action: a) adopted its May 20, March 27, and Spring National Meeting minutes; b) heard a presentation from both the Federal Bureau of Investigations (FBI) and 10-8 LLC about how they approach cybersecurity and have helped companies prepare, respond to, and recover from cybersecurity events; and 2) heard "The State of the Cyber Insurance Market: Trends, Challenges, and Opportunities," a panel discussion moderated by Commissioner Godfread, consisting of representatives of an insurer, a reinsurer, and a broker, who provided insights on the dynamic nature of cyber coverage, how it is morphing, and how cyber products differ from the typical insurance product. The panel discussed the challenge of education and awareness among consumers, industry, and state insurance regulators and how the education curve and the pace of technology changes are not always aligning.

D. E-Commerce (H) Working Group

Commissioner Downing reported that the Working Group met July 18. During this meeting, the Working Group: 1) heard a presentation from Canopy Connect on open insurance; and 2) discussed adding language to NAIC model laws to protect consumers' rights to control the usage of their information and about the work of the Privacy Protections (H) Working Group.

The Working Group also met April 4 to discuss its 2024 work plan and adopt the E-Commerce Modernization Guide.

The Working Group plans to meet in to hear a presentation from Pennsylvania on its Key Smart Launch Program.

E. Privacy Protections (H) Working Group

Commissioner Beard reported that the Working Group met Aug. 14 and took the following action: 1) adopted its Spring National Meeting minutes; 2) heard an update from NAIC staff on federal privacy legislation; 3) heard a presentation from Consumers' Checkbook on legacy systems in the protection of consumers privacy; and 4) discussed its next steps, which included the announcement of a new chair draft revising Model #672. The chair draft was announced to Working Group members and interested state insurance regulators during the Aug. 5

regulator-only call. The draft was distributed to Working Group members and interested state insurance regulators the same day to give time to review the draft prior to exposure following the Summer National Meeting. The draft will be exposed Aug. 19 for a 30-day public comment period ending Sept. 18, and the Working Group will send drafting group guidelines to start the drafting group process.

Commissioner Beard said the Working Group also met June 12. During this meeting, the Working Group took the following action: 1) heard comments from Working Group members, interested state insurance regulators, and interested parties on whether to revise the existing *Privacy of Consumer Financial and Health Information Regulation* (#672) or continue with the *Insurance Consumer Privacy Protections Model Law* (#674); and 2) discussed the comments and voted to move forward with revising Model #672, emphasizing to all interested parties that there would be sufficient time to discuss the specific privacy protections and core principles to be included in the amendments to Model #672 in the future.

During its July 10 meeting, the Working Group emphasized the importance of transparency throughout the process and that the discussion around core privacy principles and protections would be open and collaborative regardless of the framework used. On July 9, Working Group leadership met with 20 consumer representatives to hear comments providing insights on the issues most important to consumers.

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

Director Dunning reported that the Working Group met Aug. 13 and took the following action: 1) heard a presentation from McKinsey & Company on the U.S. insurance markets, including challenges in that marketplace that the InsurTech community will be able to assist insurers with, and how InsurTechs may be able to assist policyholders with more product innovation, customer experience, and streamlining manual processes in the insurance value chain; and 2) heard presentations from ClearCover, Lemonade, and Next Insurance, which are all part of the InsurTech Coalition.

G. AI Systems Evaluation and Training Collaboration Forum

Commissioner Ommen reported that following the adoption of the bulletin concerning the use of AI systems, a small group of state insurance regulators has been meeting to discuss AI evaluations, anticipating that a public discussion will commence soon after the Summer National Meeting and recognizing that this work will involve collaboration with the Market Regulation and Consumer Affairs (D) Committee. The Accelerated Underwriting (A) Working Group has completed the development of a tool as well as a regulatory outline, which, along with the Casualty Actuarial Statistical (C) Task Force work products, are likely to serve as a useful foundation for the Collaboration Forum’s work. Commissioner Ommen noted the importance of developing proposed charges and said he looks forward to public engagement in the discussions.

H. Data Call Collaboration Forum

Schultz reported that the Collaboration Forum started last year to discuss how to tackle technology and data that state insurance regulators have access to. The Collaboration Forum started with regulator-only discussions with NAIC staff, and it is anticipated to have more public discussions going forward as it develops charges. The work is in its early stages, and the Collaboration Forum looks forward to receiving public input.

I. SupTech Roundtable

Boone reported that the SupTech Roundtable was formed to review how technology can streamline and automate manual tasks in the workplace. Over the past few months, the group has been given demonstrations from Microsoft, Amazon, and Salesforce. During those demonstrations, the vendors showed their technologies and discussed the applicability of streamlining manual processes. For instance, Salesforce demonstrated its platform for case management, Slack, which could help state insurance regulators collaborate during a disaster response. Microsoft demonstrated its AI capabilities enabled in Word, PowerPoint, and Teams to summarize long documents and how to configure its AI bot to have different moods and limits on sources from which to pull data. This month, Google will provide a demonstration. Plans for future demonstrations include other big tech companies such as Adobe, Docusign, and Oracle. The SupTech Roundtable is looking into how to utilize AI overlaid into the System for Electronic Rates & Forms Filing (SERFF).

Amann made a motion, seconded by Commissioner Lara, to adopt the following reports: Third-Party Data and Models (H) Task Force; Big Data and Artificial Intelligence (H) Working Group (Attachment Two); Cybersecurity (H) Working Group (Attachment Three); E-Commerce (H) Working Group (Attachment Four); Technology, Innovation, and InsurTech (H) Working Group (Attachment Five); Privacy Protections (H) Working Group (Attachment Six); AI Systems Evaluation and Training Collaboration Forum; and Data Call Collaboration Forum. The motion passed unanimously.

3. Heard a Presentation on Federal Regulatory Actions Related to the Use of AI

Paige Waters (Locke Lord LLP) presented a review of federal tools for regulating AI. She identified the regulatory tools, compared the federal agency tools with insurance regulatory tools, and identified additional regulatory tools that insurance regulators may want to explore. She initially observed that based on current federal AI initiatives, state insurance regulators are utilizing most of the available AI regulatory concepts, but given the rapid development of AI, insurance regulators likely will benefit from monitoring federal AI initiatives. She stated that there is currently no comprehensive federal law that universally regulates AI, which has resulted in piecemeal regulation. Both the federal and insurance regulation agencies rely heavily on existing laws, use principles-based methodologies, and call for a balanced approach between promoting innovation and protecting consumers.

Federal agencies regulating financial services are further along in the development of AI regulation. Frequently used tools to help in the financial regulation of AI include written guidance, corporate governance policies, and internal controls. She noted that the U.S. Securities and Exchange Commission (SEC) is using AI red-teaming to determine flaws or vulnerabilities in the use of AI and using examinations to regulate AI. The Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC) have been involved in enforcement actions where they have levied penalties and fines against regulated entities for violations of their AI regulations. She stated that federal agencies use two additional tools: the requirements to avoid conflicts of interest and disclosures and model forms. Regulated entities must make disclosures to consumers using AI products and annual disclosures on the amount of resources they are dedicating to AI risk management and how far along they are in their compliance.

One area where federal agencies are doing something slightly different than state insurance regulators is in creating offices of technology within federal agencies, for example, the Financial Industry Regulatory Authority (FINRA), which provide subject matter expertise to the regulated entities. Both state insurance regulators and federal regulators are well-served by continuing to monitor new technological developments, new laws enacted, and case law in order to keep up with the most effective methods in regulating the industry.

Commissioner Gaffney asked about the overlap of explainability and disclosure, what key differences Waters sees between federal and insurance regulators, which of those differences insurance regulators should keep in front of, and how they should be reconciled. Waters replied that keeping up with the changes in regulatory actions will help prevent falling through the cracks.

Commissioner Ommen commented that one area where the state insurance regulatory system takes action that the federal regulators do not is that under the Own Risk Solvency Assessment (ORSA), and more generally in financial analysis, state insurance regulators have routine exchanges with insurance companies and raise these issues as part of that interaction process. He asked whether Waters sees that at the federal level in her study. Waters responded that she believes the creation of the technological offices within federal agencies is designed to provide a forum for entities to voluntarily go to the regulators on compliance issues.

Commissioner Gaffney asked Waters about her perspective on executable testing requirements and metrics. Waters responded that testing is an area that many in the insurance industry have questions about. It is an easier conversation to the extent the industry has engaged its own data scientists to help them understand some of the testing requirements. While some of those testing requirements may have initially seemed onerous, the tests are not as onerous once data scientists are involved. The education and involvement of more technical expertise in those areas have helped.

4. Heard a Presentation on NIST AISIC Efforts to Develop a Framework for Governing AI

Dale Hall (Society of Actuaries—SOA) presented an overview of some of the research and activities the SOA has been focusing on regarding the development of a framework for governing AI. He noted that the SOA was selected earlier this year to be part of a U.S. group formed by the U.S. Department of Commerce (DOC) through the National Institute of Standards and Technology (NIST) called the AI Safety Institute Consortium (AISIC). Key AISIC initiatives include a working group focused on the capability evaluation of safe AI testing and auditing and a working group focused on safety and security. Hall noted that the SOA has ongoing interaction with the AISIC working groups and that the SOA provided comments on the implementation of a generative AI risk management framework. Hall concluded by stating that the U.S. actuarial profession is strongly engaged with the rapid evolution of AI, the actuarial profession has expertise in risk management and governance, there are professional development and education opportunities on the responsible use, building, and implementing AI models, and that the U.S. Actuarial Standards of Practice (ASOPs) and Code of Professional Conduct can provide additional guidance.

5. Heard a Presentation on IAA Efforts to Survey Global AI Governance Frameworks

Andrews reported on some of the findings from the International Actuarial Association's (IAA's) efforts to review AI governance frameworks from Australia, Canada, China, Europe, Singapore, the United Kingdom (UK), and the U.S. for similarities and differences and stated that the U.S. fares well compared to the other countries in regard to AI governance. She noted that Singapore does not significantly mention governance of third-party AI systems, and China does not significantly mention bias in its framework. She then focused on the EU AI Act because it is extensive, and reviewed the four levels of risk: 1) unacceptable risk (e.g., manipulation of human behavior/classification of people based on their social behavior); 2) high risk (e.g., recruitment); 3) limited risk (e.g., impersonation/chatbots); and 4) minimal or no risk (e.g., predictive maintenance). She discussed the sustainable development goals of the AI for Good Conference held May 30–31, which included promoting AI to advance health, climate, gender, inclusiveness, prosperity, sustainable infrastructure, and other global development priorities.

Andrews also discussed the launch of NIST's Assessing Risks and Impacts of AI (ARIA) program to assess the societal risks and impacts of AI systems, where the goal is to help organizations and individuals determine whether a given AI technology will be valid, reliable, safe, secure, private, and fair. ARIA helps to operationalize the NIST framework's risk management function by recommending that quantitative and qualitative techniques be used to analyze and monitor AI risks and impacts. ARIA will help assess risks and impacts by developing a new set of methodologies and metrics to quantify how well a system maintains safe functionality within societal contexts. NIST will be looking for external partners, and the NAIC will be on the list to learn more about what it is doing. Andrews mentioned the U.S. Department of the Treasury (Treasury Department's) request for information (RFI)

on the uses, opportunities, and risks of AI in the financial services sector to better understand how AI is being used within financial services, as well as the opportunities and risks.
Andrews also discussed the bipartisan bill introduced by Rep. French Hill (R-AR) that proposes legislation to encourage financial firms to experiment with AI to develop products and services by providing some protection from regulation.

Commissioner Gaffney asked whether Andrews has seen disagreement or contention between countries. Andrews responded that the correlation versus causation issue would be significant, and model risk management to determine what constitutes algorithmic harm may not be fully flushed out.

Commissioner Gaffney asked whether Andrews had any further insights on NIST's ARIA program, particularly how it obtains protected class information to perform outcomes testing. Andrews responded that because the ARIA program is new, very little information about it is available online.

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

SharePoint/NAIC Support Staff Hub/Member Meetings/H CMTE/2024_Summer/H-Minutes/Minutes-H-Cmte081524.docx

Draft: 8/11/24

Innovation, Cybersecurity, and Technology (H) Committee
Virtual Meeting
June 28, 2024

The Innovation, Cybersecurity, and Technology (H) Committee met June 28, 2024. The following Committee members participated: Kathleen A. Birrane, Chair (MD); Chlora Lindley-Myers, Co-Vice Chair, represented by Cynthia Amann (MO); Kevin Gaffney, Co-Vice Chair (VT); Ricardo Lara represented by Ken Allen (CA); Michael Conway (CO); Michael Yaworsky represented by Anoush Brangaccio (FL); Gordon I. Ito represented by Kathleen Nakasone (HI); Ann Gillespie represented by C.J. Metcalf (IL); Doug Ommen and Daniel Mathis (IA); Jon Godfread represented by Colton Schulz (ND); Judith L. French, Matt Walsh, and Rodney Beetch (OH); and Michael Humphreys (PA). Also participating were: Kris Hathaway (AR); Wanchin Chou (CT); and Jake Martin (MI).

1. Heard Opening Remarks

Commissioner Birrane provided opening remarks noting that this meeting was part of an ongoing commitment to engage with consumer representatives, allowing them to offer perspective on the important policy discussions taking place under the Innovation, Cybersecurity, and Technology (H) Committee.

Commissioner Birrane also announced that she would retire July 1 from the Maryland Insurance Administration (MIA) and return to private practice. She then announced the following leadership changes: 1) Commissioner Gaffney will move into the chair role for the Committee, and Commissioner Conway will return to the vice chair role; and 2) Commissioner Humphreys will move into the chair role, and Commissioner Gaffney will move into the vice chair role for the Big Data and Artificial Intelligence (H) Working Group.

Commissioner Birrane also shared that Karrol Kitt (Consumer Representative) passed away June 27. Peter Kochenburger (Southern University Law School) provided further comments to acknowledge Kitt's passing and expressed gratitude for her work and support.

2. Adopted its Spring National Meeting Minutes

Commissioner Gaffney made a motion, seconded by Commissioner Conway, to adopt the Committee's March 18 minutes (*see NAIC Proceedings – Spring 2024, Innovation, Cybersecurity, and Technology (H) Committee*). The motion passed unanimously.

3. Received an Update on its Workstreams

Miguel Romero (NAIC) provided an update on the Committee's initiatives, which included progress and developments on the following workstreams:

A. AI Systems Evaluation and Training Collaboration Forum, where charges are in development anticipating the evaluation work proceeding under a new working group. This Collaboration Forum will broadly examine how state insurance regulators update market conduct processes for artificial intelligence (AI) systems.
B. Third-Party Data and Models (H) Task Force will have its next meeting July 10, with Commissioner Conway also acknowledging a meeting scheduled for July 30.

C. Big Data and Artificial Intelligence (H) Working Group is in the process of developing the health AI/machine learning (ML) survey and AI training content for state insurance regulators and is actively monitoring and supporting the adoption of the NAIC Model Bulletin by the states. This Working Group will consider the next steps after bulletin adoption.
D. Privacy Protections (H) Working Group will hold its next meeting July 10 to continue discussion on the drafting direction and engage with stakeholders and consumer representatives to solicit input.

4. Heard Presentations from Consumer Representatives

A. Consumer Protection Proposals

Brendan Bridgeland (Center for Insurance Research—CIR) noted the importance of establishing testing and monitoring programs to mitigate the potential negative impact of unfair discrimination on protected classes. He addressed additional consumer concerns about broader risks of unfair discrimination that can be created by using multiple datasets to make underwriting or rating decisions that impact consumers, as the datasets may not have had sufficient testing. He raised a concern that risk factors might be applied more than once from the combination of the datasets. He highlighted the potential concern that just because data appears to correlate with the predicted risk of loss does not guarantee that a risk classification accurately and fairly measures a risk distinction between consumers. Bridgeland noted that risk classifications can overlap or prove to be duplicative proxies of another risk factor already incorporated elsewhere; the more data elements being used, the higher the likelihood there will be potentially duplicative or overlapping data. Bridgeland cited a historical case where individuals who were either very heavy or very lean in relation to their height were charged a higher risk premium when, in fact, it was subsequently determined by actuarial analysis that smoking was the contributing factor to higher mortality, not necessarily weight. However, factors for smoking and extreme weight deviations were both being applied, in effect twice for the same risk.

Bridgeland recommended that outcomes should be tested to ensure actuarial soundness and recommended a robust spot-check of the impact of outcomes on consumers. He emphasized the importance of transparency and noted that the criminal record history of consumers can be problematic. Bridgeland said that just because a data set appears to be correlated with predictions of loss does not guarantee that a particular risk classification accurately and fairly measures a distinction between two consumers. He further noted that the more disparate factors are used without considering the causation element, in particular, how those factors might interact and lead to a result or even interfere with each other in a manner that might lead to unfair discrimination.

Bridgeland highlighted the importance of transparency for consumers to trust the insurance industry. He noted that every time a consumer learns about a new industry practice affecting them, and they learn about it for the first time through a cancellation notice or a salacious media article, it harms the reputation of insurers and state insurance regulators.

Kochenburger added that consumers cannot evaluate this issue for themselves and that it is almost impossible to access their own information and how it is being used. These evaluations require an analysis of the pooled data on a systematic basis to identify bias. He noted that this could be done through litigation class action suits eventually but is not the preferred method.

B. Privacy Protections

Brenda Cude (Consumer Advocate) stated that the primary goal of privacy protections regulation is to control personal consumer data collection, processing, and transfer (i.e., the goal should be to strengthen existing protections regarding this information). She expressed concern that it is impractical for consumers to be counted on to protect themselves due to the constant monitoring of multiple organizations that constantly change their policies. Cude said most consumers lack the time and expertise required to exercise their privacy rights and do not have the ability to assess the risk from organizations that have access to their data. She noted that one academic study estimated that it would take a typical person 200 hours a year to read all the privacy notices relevant to them, assuming the notices were even readable. She noted the additional difficulty in assessing the increasing risk of data privacy in light of advancements in AI, which could cause a collective social problem. Cude said she expects regulation that emphasizes data minimization, clear expectations about the policies and procedures required to dispose of personal information when it no longer serves a business purpose, timely and transparent consumer notices, prohibitions on insurers discriminating against consumers who opt out of disclosing personal information, and an opt-in rather than opt-out approach. She concluded by stating that a privacy rights-based approach simply puts too much responsibility on individuals to solve a problem that is not an individual problem but rather one shared by all consumers.

Harry Ting (Health Care Consumer Advocate) stated that the passage of a new privacy model should be a priority of the NAIC. He brought to light that expecting consumers to read privacy policies, which are difficult to understand, in order to provide the consumer's choice to opt out of sharing personal information is not effective protection. He noted that the *Insurance Consumer Privacy Protection Model Act* (#674) states that "No licensee shall collect, process, or share a consumer's personal information in connection with any additional activity without first providing the consumer a clear and conspicuous notice that such information will not be collected, processed or shared unless the consumer opts in to such collection and use their personal information," and that such a provision must be included in the new privacy protection model. Additionally, Dr. Ting said that protected consumers must include not just current customers but also insurance applicants and past customers. He added that currently, many privacy policies claim to protect consumer privacy but use dark pattern techniques that make it difficult for consumers to do so, which is why the Working Group should create a template privacy policy for licensees. Dr. Ting said the U.S. Department of Health and Human Services (HSS) has used this approach for years to communicate with Medicare Advantage and Part D drug plan customers. He said the template should use the informational categories that California requires.

Dr. Ting, speaking for Erica Eversman (Automotive Education & Policy Institute—AEPI), continued by stating that third-party service providers must follow privacy policies when they are provided data and that without this requirement, personal information is not protected. He said providing undefined blanket statements about privacy protection policies that third-party service providers must follow is useless. Further, he stated that the model that the Privacy Protections (H) Working Group develops must require licensees to explicitly explain what privacy practices the third-party service providers must follow and should define those provisions accurately and with proper limitations. The new privacy protection model needs provisions requiring data minimization and deletion of information that is no longer needed.

Lucy Culp (Leukemia & Lymphoma Society—LLS) stated that the use of AI systems poses significant risks to consumers by reinforcing long-standing biases to consumers, and there is a need to ensure that the health AI/ ML survey addresses the ways that AI is used in health insurance by including more granular questions than those included in the life AI/ML survey. She recommends questions focused on the benefits and usage of AI and noted that the role of third parties is more pronounced than in life insurance. She further stated that there is a greater need to understand how underlying datasets are used, and more granular questions are needed to better understand how insurers are monitoring the quality of datasets aggregated by third-party providers because the way they are integrated could be problematic. Culp stated that consumer representatives should have the opportunity to review the survey in a testing/pilot phase. She said that a unique feature of health insurance is the interaction within the medical system and that insurers are increasingly relying on AI to supplement or supplant individual decision-making and the judgment of medical professionals and prior authorization or even levels of care assessment or other coverage determinations. She recommended following a similar procedure that the federal Centers for Medicare & Medicaid Services (CMS) has implemented, which is to prohibit Medicare Advantage plans from solely relying on the use of AI to make coverage determinations or terminate service. She recommended that the Committee and individual states consider this policy. Culp additionally noted that the HHS Office of Civil Rights (OCR) recognizes the important role of AI in health programs and activities in its recently finalized regulations, implementing Section 1557. In that new rule, the HHS OCR is requiring covered entities to make reasonable efforts to identify the use of AI tools and to mitigate the risk of discrimination resulting from how those tools are used.

Adam Fox (Colorado Consumer Health Initiative—CCHI) reiterated that there is a need to critically approach the issue of using AI. He expressed concerns regarding whether there are clear benefits to patient outcomes and whether privacy and concerns of potential bias and discrimination are adequately addressed. He noted that women and people of color may be biased against due to limited representation in data sets and that AI systems must be designed from the ground up in order to mitigate perpetuating and reinforcing inequalities to prevent unintended consequences and bias. Appropriate quality and representative data must be used, and the design of the algorithms and models must be suitable for intended use to prevent bias and discriminatory assumptions. He continued by stating that it is important to ensure the same level of governance and accountability applies to third-party vendor models that may be used in insurance practice. Fox said that carriers who effectively manage both coverage and providers or hospital systems through integrated health maintenance organizations (HMOs) may leverage additional applications of AI and algorithms in the provision of healthcare services and management of claims or utilization, which adds a layer of complexity to the already significant risks for discrimination and inappropriate denials of care.

Commissioner Birrane then solicited questions from members of the Committee and its Working Groups, to which Commissioner Gaffney expressed appreciation for the adoption of the Model Bulletin and looked forward to continuing to work with the consumer groups to ensure a good outcome to protect consumers. Commissioner Birrane pointed out that during the Committee’s session at the Summer National Meeting in Chicago, there will be a panel presentation on the use of AI in health care.

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

SharePoint/NAIC Support Staff Hub/Member Meetings/H Cmte/2024_Summer/H-Interim-Meeting062824/Minutes-H-Cmte_062824.docx

Draft: 8/26/24

Big Data and Artificial Intelligence (H) Working Group
Virtual Meeting
July 29, 2024

The Big Data and Artificial Intelligence (H) Working Group met July 29, 2024. The following Working Group members participated: Michael Humphreys, Chair and Shannen Logue (PA); Kevin Gaffney, Vice Chair and Mary Block (VT); Jimmy Gunn (AL); Alex Romero and Molly Nollette (AK); Tom Zuppan represented by Lori Munn (AZ); Ken Allen (CA); Michael Conway represented by Jason Lapham (CO); Andrew N. Mais represented by George Bradner (CT); Karima M. Woods (DC); Rebecca Smid (FL); Weston Trexler (ID); Erica Weyhenmeyer (IL); Amy L. Beard represented by Victoria Hastings (IN); Doug Ommen represented by Jared Kirby (IA); Tom Travis (LA); Sandra Darby (ME); Raymond Guzman (MD); Caleb Huntington (MA); Jeff Hayden and Jake Martin (MI); Jacqueline Olson and Phil Vigliaturo (MN); Cynthia Amann (MO); Connie Van Slyke (NE); Scott Kipper represented by Nick Stosic (NV); Christian Citarella (NH); Adrienne A. Harris represented by Kaitlin Asrow (NY); John Harrison represented by Tracy Biehn (NC); Jon Godfried represented by Colton Schulz (ND); Judith L. French represented by Matt Walsh (OH); Elizabeth Kelleher Dwyer (RI); Michael Wise (SC); Carter Lawrence represented by Emily Marsh (TN); J'ne Byckovski and Rachel Cloyd (TX); Scott A. White represented by Dan Bumpus (VA); Nathan Houdek represented by Lauren Van Buren (WI); and Bryan Stevens represented by Lela Ladd (WY).

1. <u>Adopted its Spring National Meeting Minutes</u>

Commissioner Gaffney made a motion, seconded by Superintendent Dwyer, to adopt the Committee's March 16, minutes (*see NAIC Proceedings – Spring 2024, Big Data and Artificial Intelligence (H) Working Group*). The motion passed unanimously.

2. <u>Received an Update on the Working Group's Health Insurance AI/ML Survey Work</u>

Commissioner Humphreys provided an update on the status in the development of the health insurance AI/ML surveys, which included tailoring the prior surveys' questions to health insurance, proceed with a pilot study, and issue the survey later this year. He reiterated that the purposes of the health AI/ML surveys are to understand how industry is using AI, how the use of AI is governed, and how the products and systems are being developed to guide future discussions on next steps. Commissioner Humphreys stated that the group has had some conversations with consumer representatives and are currently finalizing conversations with a handful of large major medical carriers that will participate in the pilot program to give feedback on the survey questions. By the Spring National Meeting the group will have the analysis and report complete for discussion at the group level and publicly.

Birny Birnbaum (CEJ) asked what the plan was for reissuing the surveys to receive updated responses. Commissioner Humphreys deferred this question to Shannen Logue (PA) to answer.

Josh Goldberg (HCSC) asked to confirm that the launch of the survey is planned for November 11 with a due date of January 15. Commissioner Humphreys confirmed.

Shannen Logue (PA) stated the group met with consumer representatives on May 13 to receive feedback and stated that the survey will be issued for public access on October 4. She stated that the health surveys will include questions relating to data usage, arrangements with third parties, coordination of governance with existing health provider governance standards, and will be tailored to the use of AI in operational functions of health insurers. She explained the group's intentions are to ensure that the questions align with the NAIC Model Bulletin.

Regarding the auto surveys, the group will conduct regulator-only follow up discussions with selected personal auto carriers. Among those carriers, for those that initially responded that they do not currently use AI/ML in their operations, the group will follow up to ask whether they have begun to use AI or ML in which operations and in which capacity. For the selected carriers that originally responded they are currently using AI/ML, follow up questions will be asked about any changes in their use of AI/ML, whether they have begun to use generative AI, their degree of human involvement, efforts to identify and mitigate model drift, and their uses of third-party systems. The group anticipates completing the first round of follow up interviews by October 31 and anticipates repeating the surveys every two to three years.

Birnbaum asked whether the plan consists of following up with selected companies who provided anomalous responses between auto and home who indicated that they have certain uses or that they were engaged in using AI/ML. Logue confirmed that is correct. Birnbaum expressed that repeating the surveys on a regular schedule would result in more consistent responses.

Lucy Culp (Leukemia & Lymphoma Society) asked whether Other Health, like Short Term Plans Accepted Benefits, will be included in the surveys. Logue responded that the surveys will start with comprehensive major medical plans (individual, the small group, large group as well as student health), but then there could be a second round of surveys.

3. Received a Presentation on the Society of Actuaries' Research on Inference Methods

Dorothy Andrews (NAIC) covered several aspects of the Society of Actuaries (SOA) paper on inference methods, explained the theory of the BIFSG method, and included examples of the results of the method. Andrews discussed the underlying data used by the BIFSG method, its limitations, and concerns regarding its accuracy. She showed how the BIFSG method has been applied to a variety of studies and applications, including health care decision making, mortgage and non-mortgage lending patterns, academic research, taxation, and financial credit access issues. She explained a few of the performance metrics used, and introduced the concepts of the probabilistic and statistical types of inference methods. She clarified that the BIFSG method is a Bayesian probabilistic approach. She explained that the BISG only uses surnames, geo-location, and census bureau demographics data to estimate race, while the BIFSG additionally uses first names to estimate probabilities of race and ethnicity. The BIFSG method has been applied on data from mortgage applications and voter registration rolls and has shown improvement over the BISG method in accuracy and coverage. The BIFSG method was used to find that the incidence of missing race and ethnicity data is higher among non-Hispanic and Hispanic blacks than other groups.

Andrews then walked through the mechanics of how the probabilities are calculated in the BIFSG method using Bayesian theory, and provided the results of estimated probabilities of race for Miguel Romero (NAIC), Scott Sobel (NAIC), and herself. She explained why her estimated race was incorrect considering her first and last names and her location of residence. In that example, she provided insights into how bias can be embedded in reference/training data. She provided another example that referenced a study where the researchers found the BIFSG method overestimated the earned income tax credits take-up rate for whites, and underestimated the rate for blacks; it underestimated average tax rates for whites but was fairly accurate for blacks, Hispanics, and other groups; and it predicted higher audit rates for whites than non-whites, which is in conflict with actual audit rates. She clarified that the BIFSG method was designed to perform inference on a large group of people, not to infer the race at an individual level.

Sylvia Yee (DREDF) asked about whether the method would work well on people of mixed race. Andrews responded that the method may not be as accurate on people of mixed race, and for people who live in very diverse communities.

Birnbaum commented that perfect is the enemy of good, in that there is a technology that has been used in regulatory applications that, while may not be perfect, may be fit for purpose to assess bias in AI applications and insurance applications. Further he stated that while there is always room for improvement, there is no reason for the NAIC not to endorse testing for racial bias using the BIFSG method.

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

SharePoint/NAIC Support Staff Hub/Member Meetings//H CMTE/2024_Interim Meetings/Minutes-BDAIWG072924.docx

Draft Pending Adoption

Draft: 8/28/24

Cybersecurity (H) Working Group
Chicago, Illinois
August 14, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Chicago, IL, Aug. 14, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair, and Eric Lowe (VA); Bud Leiner (AZ); Chris Erwin (AR); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Elizabeth Nunes and Matt Kilgallen (GA); Lance Hirano (HI); Daniel Mathis (IA); C.J. Metcalf (IL); Craig VanAalst (KS); Mary Kwei (MD); Jeff Hayden and Jake Martin (MI); Jacqueline Olson and T.J. Patton (MN); Tracy Biehn (NC); Jon Godfread and Colton Schulz (ND); Christian Citarella (NH); Nick Stosic (NV); Gille Ann Rabbin (NY); Matt Walsh (OH); Mike Humphreys and David Buono (PA); Andrea Davenport (WI); and Lela Ladd (WY). Also participating were Sheila Travis and Mark Fowler (AL).

1. Adopted its July 9 Minutes

The Working Group met July 9 (Attachment Three-A). During this meeting, the Working Group took the following action: 1) adopted its May 20, March 27, and Spring National Meeting minutes and 2) heard a presentation from the Federal Bureau of Investigation (FBI) and 10-8 LLC on their approach to cybersecurity incidents.

Chou made a motion, seconded by Schulz, to adopt the Working Group's July 9 (Attachment Three-A) minutes. The motion passed unanimously.

2. Heard a Panel Discussion on the State of the Cyber Insurance Market

Moderated by Commissioner Godfread (ND), the panel, titled "The State of the Cyber Insurance Market: Trends, Challenges, and Opportunities," featured three industry experts: Brent Rieth (Aon), Jamie Schibuk (Arch Insurance), and Shawn Ram (Coalition). Structured in four key areas, the discussion covered 1) market trends, 2) coverage, 3) risk management and claims, and 4) regulatory matters.

Starting with the state of the cyber insurance market, Commissioner Godfread asked Rieth to describe the market and how it has evolved over the past five years. Rieth explained the market evolves with the constant barrage of new and different risks, and insurance companies are trying to navigate developing products and how to do it in a sustainable way on a long-term basis. Addressing the second part of the question, Rieth mentioned how in 2019, the industry observed a significant volume increase of claims connected to ransomware activity where criminals, motivated by monetary gains, attacked companies through the encryption of data and systems, making it difficult for businesses to operate. From 2021 to 2022, the industry saw a dramatic change in how product was priced and an evolution in how it was structured, and in some instances, this meant higher retention levels. An evolution in policy wording around ransomware occurred, as insurance carriers looked to manage the accumulated losses from the 2019 era. Beginning in 2023 and throughout 2024, the pricing environment has increased in competition, as new entrants came into the marketplace, expanding buyer options. Coverage also continues to evolve specifically around the topic of war and the rigorous underwriting process, and how companies are reviewed has become more comprehensive.

Commissioner Godfread opened the question to the remaining panelists. Ram went further back in time back to 2012 which he referred to as the year of the breach in the cyber world, as Target, Home Depot, and other companies lost hundreds of millions of records. The nature of what cyber insurance was then and continues to be today is focused on the notion of data breach. From an underwriting standpoint, there is an understanding of the amount of records a company has, the resulting impact of a breach, and the cost to remediate. This evolved through more of a focus on business email compromise and security deficiencies, where attack vectors associated with email led to funds being transferred fraudulently to the proliferation of ransomware. Ram said to mitigate the trend of ransomware, the underwriting community emphasized the importance of two-factor authentication, the significance of segmented backups, and a variety of other security measures. The insurance industry helped aid companies around the world to improve their security to maintain insurability, specifically around ransomware, and as security improved, the interest in cyber increased.

Schibuk explained his observations of the shift in underwriting: the level of scrutiny and volume of questions increased. This sophistication in underwriting increased the understanding of what drives claims. He described the emergence of technology to conduct external and internal scans to give a better sense of security posture, which has led to insurers working with the insureds in a more consultative manner.

Referencing the panel's discussion of security package improvements, Amann mentioned reports of a Pakistan-based hacking group that used emojis instead of standard patch language to get around the standard patch security. It was described as "clever on the part of the hackers." Ram explained that Coalition uses a few hundred virtual machines across the world to mimic policyholder technology, reporting over 100 million attacks on these honeypot machines in the previous seven days and giving insights into the mechanisms the cyber actors are utilizing to infiltrate an organization. If there is a concentration of malware, Coalition can develop the decryption cable to help policyholders be prepared.

Commissioner Godfread explained that the cyber market penetration is limited compared to other commercial or personal lines. He asked Ram to explain his opinions on why there is limited penetration and to touch on the biggest impediments to future growth of the market. Ram explained that the Standard & Poor's 500 index (S&P 500) asset class in 1980 would have been focused on tangible property, such as boilers, machinery, and buildings. The same cohort of companies today would be almost exclusively focused on intangible assets, such as intellectual property and trade secrets. Describing the fourth industrial revolution, the digital transformation, Ram said the nature of insurance products has not evolved in the same fashion as asset classes. The nature of impediments revolves around education and a limited understanding of the industry around digital or cyber risk. Ram said this year has been interesting in the world of cyber risk in the United States. In February, Change Healthcare had two-thirds of pharmacists, clinics, and other health-care-related companies impacted by a particular piece of technology. CDK Global impacted 15,000 auto dealerships across North America. Many auto dealerships did not understand the nature of how one piece of software could take down their ability to sell cars and how that could be covered in a cyber insurance policy. He said breaches of this type can improve education among consumers because it helps them understand the risks they might be experiencing.

Accentuating the nuance of the small- and medium-sized entities (SME), he said there is a convergence of misunderstanding of what cyber insurance is and a misunderstanding of what adversaries do. SMEs often believe adversaries are focused on large companies, looking for revenue. Ram said while that may be the greatest impediment, the industry needs to provide education. Schibuk said when using the carrier perspective to look at the low market penetration rates today, projecting outgrowth over a five- to 10-year period results in a fairly sizable marketplace. As the industry grows, continuing to get reinsurers and third-party investors familiar with the cyber risk class will be important. Rieth explained that since cyber is a newer coverage for a lot of companies, it does take work to familiarize them with it and get into a position where they see enough value to purchase the coverage. It is important to consider both the pace at which the risks are changing and the pace at which the industry can change the product itself. There are some policies that can address systems failure or technology outage; however, it is not understood by every company purchasing, and in some instances, they just purchase the minimum.

Citarella asked the panel to discuss the extent to which the underwriting process is crafted to the needs of the individual and to what extent a loss cost comparison between policies is possible. Rieth described that while there is some level of off-the-shelf policies, there are also a lot of variances across carriers in terms of base level of coverage. This puts pressure on brokers and agents to have knowledge and review the variations in policy wordings and identify needs for improvements, which is not done consistently across segments or geographically if the company is larger.

Chou asked the panel to discuss how cryptocurrencies and artificial intelligence (AI) will affect cyberattack trends. Schibuk explained that the industry has seen threat actors using AI in their applications to scale their operations more efficiently, potentially allowing them to conduct more widespread attacks. Equally, leveraging AI on the defense side, Ram described how Coalition tracks adversarial activity, allowing AI to process the data to aid in developing defensive mechanisms. Regarding cryptocurrencies, Ram suggested that regulations will have an impact on trends, as more organizations refuse to accept the challenges in tracking the money.

Commissioner Godfread asked Ram to discuss some of the common exclusions and how the market is responding. Ram explained how the conflict in Russia and Ukraine has resulted in the war exclusion in cyber, materially impacting the belief of cyber coverage value to some larger companies. These larger companies believe they could be the victim of a nation-state attacker. Additionally, Ram explained there are common exclusions or lack of coverage for items such as funds transfer fraud liability, which can be impactful depending upon the type of company.

Commissioner Godfread asked Rieth to comment on Aon's report of the lack of consistency in the market regarding exclusionary language. Rieth explained how the London marketplace responded to guidelines set by Lloyds of London with 43 variations of compliant wording of one exclusion. This introduced a learning curve for insurers to understand the language being proposed. It also highlighted the concern of accumulating risk that might arise from a nation-state attack.

Inquiring about a federal backstop, Amann asked if it would be viable for a catastrophic event to develop something like the Terrorism Risk Insurance Act (TRIA). Rieth said it would be important to continue to evaluate, working through the process of identifying the risk issues the insurance industry is concerned about. The solvency risk becomes a concern when the risk aggregation is so large. This should allow the insurance carriers to have a more appropriate conversation with reinsurers and the government to determine if a backstop mechanism is feasible.

Commissioner Godfread asked the panelists to give their perspectives on what regulators could do to support the marketplace. Schibuk summarized the discussion's theme as the product's evolution and the efforts that have gone into it. He said regulators should be open to innovation to drive the overall process and use data analysis to reduce risk for the policyholder. Ram suggested a degree of cognizance, being aware of how unique cyber is and how fundamentally different it is from most insurance coverages. The nature of the risks associated with homeowners insurance does not dramatically change within a policy period; however, with cyber, there can be dozens, if not hundreds, of technology updates on existing software during the same period. Ram said ongoing collaboration and regulatory support will help standardize and increase understanding of the product. Rieth said addressing the learning curve by helping to educate companies about the risk issues they face, and mitigation steps can add value to the partnerships with insurance companies. An ongoing dialogue between the regulatory and private sectors is critical.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Summer/WG-Cybersecurity/Minutes-CyberWG081424.docx

8/1/24

Cybersecurity (H) Working Group
Virtual Meeting
July 9, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met July 9, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Julia Jette (AK): Mel Anderson (AR); Damon Diederich (CA); Wanchin Chou (CT); Daniel Mathis (IA); C.J. Metcalf (IL); Shane Mead (KS); Mary Kwei (MD); Jake Martin (MI); T.J. Patton (MN); Tracy Biehn (NC); Colton Schulz (ND); Gille Ann Rabbin (NY); Don Layson (OH); Jodi Frantz (PA); Andrea Davenport (WI); and Lela Ladd (WY).

1. Adopted its May 20, March 27, and Spring National Meeting Minutes

The Working Group met May 20 and took the following action: 1) received an update on the Cybersecurity Event Response Plan (CERP); and 2) heard a presentation from CyberCube on cyber risk. The Working Group also met March 27 to hear an update from the White House Office of the National Cyber Director (ONCD) related to cybersecurity and cyber insurance.

Schulz made a motion, seconded by Peterson, to adopt the Working Group's May 20 (Attachment Three-A1), March 27 (Attachment Three-A2), and March 17 (see *NAIC Proceedings – Spring 2024, Innovation, Cybersecurity, and Technology (H) Committee, Attachment Two*) minutes). The motion passed unanimously.

2. Heard a Presentation from the FBI and 10-8 LLC on Their Approach to Cybersecurity Incidents

Ignace Ertilus (Federal Bureau of Investigation—FBI) said the presentation title, "Changing Landscape," was chosen because cyber is always changing. Just when a threat such as fraud and phishing feels handled, a new technology comes about like artificial intelligence (AI) and completely changes the threat landscape. Cyber actors categorically fall into six definitions: 1) hacktivism; 2) crime; 3) insider; 4) espionage; 5) terrorism; and 6) warfare. Historically, there was a clear distinction between the different cyber actors. Now there appears to be more of a blend. North Korea has nation-state actors, but a lot of reporting out on North Korea suggests more actors' involvement with ransomware. This is where the actors can make money for the regime and is an example of where a nation-state actor can fit into multiple categories. The crime category actors are typically after personally identifiable information (PII), which can be used to sell on websites for others to commit tax fraud or identify theft.

Of the various types of attacks, the presentation focused on ransomware, business e-mail compromise, investment scams, and tech support. Ertilus said these four types of attacks accounted for the largest losses associated with reporting to the FBI's Internet Crime Complaint Center (IC3).

Ertilus said that ransomware is a form of malware that encrypts files on a victim's computer or server. Ransomware has been around for quite some time, but around 2018, its frequency increased. Expected targets of ransomware include state and local governments and industries that need immediate access to their data, such as the health care industry. Ransomware is a tool that cyber actors use, but they are exploiting some key vulnerabilities in systems to be able to execute ransomware files. Companies have to think about what those vulnerabilities could be for their own infrastructure. In 2023, the FBI's IC3 received more than 2,800 complaints identified as ransomware with adjusted losses of approximately $60 million. Separate studies have shown 50%–80% of victims that paid the ransom experienced a repeat ransomware attack by either the same or different actors. Ertilus discussed multiple defensive best practices, including regular data backup and integrity verification, regular scans, application whitelisting, and physical and logical separation of networks. Another defensive best practice is providing awareness and training, such as teaching people within the company not to click on everything sent to them.

Ertilus said that business e-mail compromise or account compromise is one of the most financially damaging online crimes. It exploits the fact that so many people rely on email to conduct both personal and professional business. These sophisticated scams are carried out by fraudsters compromising email accounts to conduct unauthorized transfer of funds. In a business email compromise (BEC) scam, criminals send an email message appearing to come from a known source making a legitimate request, such as a company CEO asking an assistant to make a quick purchase or wire transfer. Common preventative measures include using multifactor authentication (MFA) and reviewing hyperlinks for misspellings or domain names for typos. Some companies implement multi-tier authentication for fund transfers to avoid a single point of failure in their security.

Ertilus said that investment scams are the largest cause of loss of any crime type tracked by IC3. These deceptive practices induce investors to make purchases based on false information. Investment fraud rose 38% in 2023 to $4.57 billion. Investment fraud with reference to cryptocurrencies rose from $2.57 billion in 2022 to $3.96 billion in 2023, an increase of 53%. These scams can start with a simple text message from an unknown source, designed to entice targets with the promise of lucrative returns on their investments.

Cyberthreat actors are increasingly using tech support and government impersonation avenues to target victims. In order to increase the possibility of success, threat actors introduce a sense of urgency or fear. Two examples are: 1) claiming the victim has a critical error with their computer, requiring immediate attention; or 2) alleging the victim missed jury duty in a message appearing to come from the local sheriff. In such instances, victims are inclined to the respond to avoid future issues.

Gregory Crabb (10-8 LLC) discussed the company’s “Mastering the Six Steps to Effective Threat Intelligence” program. The approach integrates threat intelligence into security strategy and focuses on understanding and countering an adversaries’ tactics, techniques, and procedures. The six steps are: 1) identify and understand the threats; 2) define intelligence needs; 3) prioritize assets and services; 4) collect and analyze information; 5) make informed decisions and communicate effectively; and 6) continuously improve the threat intelligence program.

Crabb said the benefits of this six-step cybersecurity approach are observable in the organization being ready, responsive, and resilient. Using the six steps empowers an organization to effectively anticipate and counteract cyberthreats.

Chou requested additional information regarding the 10-8 cyber arena offering, expressing interest in the opportunity.

Miguel Romero (NAIC) reminded the Working Group of its work plan for the year. He said the Working Group plans to meet with experts and understand their perspectives to shape policy discussions, as well as hear presentations on federal updates and from AM Best.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Summer/WG-Cybersecurity/Minutes-CyberWG070924.docx

Draft: 6/17/24

Cybersecurity (H) Working Group
Virtual Meeting
May 20, 2024

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met May 20, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Julia Jette (AK); Bud Leiner (AZ); Wanchin Chou (CT); Tim Li (DE); Tia Taylor (GA); Lance Hirano (HI); Daniel Mathis (IA); C.J. Metcalf (IL); Mary Kwei (MD); Jake Martin (MI); Bubba Aguirre (MN); Tracy Biehn (NC); Colton Schulz (ND); Christian Citarella (NH); Scott Kipper (NV); Gille Ann Rabbin (NY); Matt Walsh (OH); David Buono (PA); John Haworth (WA); Rebecca Rebholz (WI); and Lela Ladd (WY).

1. Heard an Update on the CERP

Peterson provided a brief update on the Cybersecurity Event Response Plan (CERP), which was adopted at the Spring National Meeting. To add background for those who need it, Peterson said the CERP is meant to assist states with implementing their own versions of the *Insurance Data Security Model Law* (#668). The long-term goal of the CERP is to act as a living document that can be updated over time to achieve convergence in the cybersecurity event response space.

Peterson discussed the difficulties included in various notification laws: Multiple departments require similar types of data to be included, but the reporting method and updating vary. The added complications are not helpful during an already stressful time. After multiple discussions, the direction is leaning toward a confidential repository at the NAIC. Additionally, similar solutions have been utilized for licensee filings of risk-based capital (RBC), Market Conduct Annual Statement (MCAS), as well as System for Electronic Rates & Forms Filing (SERFF) confidential and trade secrets filings. This type of repository would offer improved security, heightened awareness, and more confidential treatment.

Peterson stated there remains a lot of work to do, but the intent is to get a lot of agreement on this particular project and for it to be viewed as an improvement that will benefit supervisors and licensees alike.

2. Heard a Presentation from CyberCube on Cyber Risk

Amann introduced Rebecca Bole (CyberCube) and Jon Laux (CyberCube), emphasizing their cybersecurity and insurance expertise.

Bole offered the presentation as an opportunity for reflection on data, methods available, and what is being used in the insurance industry. Namely, she said she would discuss what is happening in the cyber risk landscape and how it is applied to insurance, focusing on the cyber risk the insurance industry takes.

CyberCube is a data analytics company seeking to provide analytics to quantify cyber risk for its clients. CyberCube partners with state insurance regulators, rating agencies, and government agencies to create frameworks for governance. Bole cited the company's active partnership with the U.S. Department of the Treasury (Treasury Department) as the Federal Insurance Office (FIO) seeks to understand catastrophic cyber risk in the U.S. economy to structure appropriate federal responses.

Laux presented a brief, high-level overview of the state of the cyber market, adding additional context to describe cyber risk at a conceptual level, such as in property/casualty (P/C) and terrorism. Observations indicate cyber insurance is among the most volatile P/C lines of business.

When asked to talk about the data available for underwriting, Laux said the good and bad news is that cyber risk data is everywhere. He said everything digital is tracked in a way the physical world is not. This can be frightening from a privacy point of view, but from a data point of view, there is a lot to look at. Laux said that, broadly, many underwriters are trying to use a combination of external and internal network scans. Utilizing information, they can scan a network with tools from CyberCube, SecurityScorecard, or Bitsight. Scalable intelligence can be done to look at organizations in many of the same ways those with ill intent do. If those with ill intent can see that a particular technology vulnerability is open, that is the first step in exploiting it. While challenging, there are some places this can be done. In practice, a lot of the information is obtained through underwriting questionnaires to fill in the gaps.

Laux said an important and relevant question is whether we can use the data quickly and efficiently and make sense of what trends might be coming in. Detailed analysis can inform decision-making and quantify the importance of security signals. He said CyberCube carefully reviews 40 different information signals that indicate an organization's risk posture. Once digested, the organization is given a security score of 0–100. Laux pointed out the presence of things one might call "negative hygiene," sort of the equivalent of leaving your doors unlocked if you are in an unsafe neighborhood, and everything on the internet is potentially an unsafe neighborhood. Those are important because they are signals that, while indicative that things are problematic for the organization, can be avoided. For instance, ports can be closed, and software updates can be deployed to resolve the issue. Laux stated the level of accumulation risk has grown significantly for the industry. CyberCube sees a cutting edge around the point of underwriting, looking at the marginal risk of any given policy. An organization can look at a point of underwriting, what each policy they are considering bringing on to their books does to their overall tail exposure.

Without clear public sector direction from state insurance regulators or any other group, the markets have been grappling with the challenge of knowing when things have become too big. Similar to how terrorism was kicked out of property policies after the Sept. 11, 2001 terrorist attacks, insurers are afraid of something comparable happening in the digital space. Various approaches to addressing the question have been observed through exclusions, much like critical infrastructure is often excluded. Carriers are also evaluating widespread event triggers or limits, similar to how hurricane is done. Some insurers are exploring sub-limits to contain some of their tail risk. Mitigation potential can be further extended through active risk monitoring. Developing alerts and notifications or sending additional questions to a policyholder allows for assessing where their exposures are and knowing how they are adapting to these things.

Laux offered three final points: 1) cyber insurance requires adaptiveness and ongoing engagement with policyholders to improve resilience and reduce potential claim costs; 2) there is an abundance of data available to cyber insurers for underwriting and risk management; and 3) understanding an insurer's use of data, level of testing, and adaptability to change are important criteria for underwriting maturity.

Bruce Jenson (NAIC) asked about cyber catastrophe bond issuance, particularly whether CyberCube expects more activity in this space. Laux observed four catastrophe bonds issued before Jan. 1 of this year. CyberCube was the lead modeler for three and was also highly involved in the fourth. Laux said CyberCube does think the market could adopt this. This first issue cycle was just the beginning. He said that, in many ways, CyberCube hopes this becomes a robust cap bond support for cyberspace. Bole suggested that the injection of capital markets capital and due diligence into the cyber insurance and reinsurance market is a real test and, ultimately, validation of the market's maturity. There is a high level of due diligence in the transactions, not just modeling, but the coverage, definitions, and clarity of exposure the bonds take on. This capital source is a strong positive indicator of the growth of this market.

Peterson posed a series of questions. Firstly, he asked who the typical buyer of cyber insurance is. He then asked if most buyers are relatively sophisticated businesses or if they are individuals also purchasing cyber insurance. Lastly, Peterson asked whether we expect the current buyer demographic to continue into the future. Laux answered by saying the typical buyer is an American business. Recognizing the product's rapid growth in other parts of the world, the U.S. has had the deepest penetration for insurance buyers. He provided additional observations of the largest companies beginning to purchase cyber insurance policies as far back as 2004, when privacy laws were first put in place. He said today's market has expanded to include the small business world following the ransomware trends. Based on the NAIC's own data, Laux reflected on an area of continued development between companies buying standalone cyber insurance policies and companies purchasing an endorsement of some kind.

Regarding the current mix of buyers, Laux suggested it would not be surprising to see more small organizations buying standalone insurance coverage over time, where it is efficient for the company. Individuals purchasing cyber insurance are likely to continue to be high-net-worth individuals with concerns of having something to potentially lose.

Amann offered appreciation for Bole and Laux's expertise and extended an offer for them to return for a future presentation. She also suggested the audience should expect an email regarding the CERP and provide ideas and suggestions for other speakers to participate in the Working Group's charge to provide cybersecurity and cyber insurance education.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Summer/WG-Cybersecurity/Minutes-CyberWG052024.docx

Draft: 4/16/24

Cybersecurity (H) Working Group
Virtual Meeting
March 27, 2024

The Cybersecurity (H) Working Group met March 27, 2024. The following Working Group members participated: Cynthia Amann, Chair, and Brad Gerling (MO); Michael Peterson, Vice Chair (VA); Julia Jette (AK); Chris Erwin (AR); Bud Leiner (AZ); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Elizabeth Nunes (GA); Daniel Mathis (IA); C.J. Metcalf (IL); Shane Mead (KS); Mary Kwei (MD); Jake Martin (MI); T.J. Patton (MN): Tracy Biehn (NC); Martin Swanson (NE); Colton Schulz (ND); Christian Citarella (NH); Nick Stosic (NV); Gille Ann Rabbin (NY); Don Layson and Matt Walsh (OH); David Buono (PA); John Haworth (WA); Andrea Davenport (WI); and Lela Ladd (WY).

1. Heard an Update on White House ONCD Activities Related to Cybersecurity and Cyber Insurance

Amann introduced Stephen Viña, Senior Advisor with the Office of the National Cyber Director (ONCD) of the White House. Viña noted that the ONCD helps monitor threats and coordinate responses.

Viña provided an overview of the ONCD's activities, including a briefing on the contents and intent of the National Cybersecurity Strategy.

Viña noted that the development of the National Cybersecurity Strategy included consultations with interagency and external stakeholders and built on previous strategies, including President Biden's work of the prior two years. The goal is to have a digital ecosystem that is more defensible and resilient.

Viña said the strategy represents a fundamental shift in rebalancing the responsibility to defend cyberspace and realigning incentives to favor long-term investments. The National Cybersecurity Strategy is organized around five pillars, which include: 1) defending critical infrastructure; 2) disrupting and dismantling threat actors 3) shaping market forces to drive security and resilience; 4) investing in a resilient future; and 5) forging international partnerships.

The ONCD published an implementation plan July 13, 2023, including 69 initiatives, each with a singular, responsible agency and a completion date. The expectation is that the implementation plan will be updated at least annually, with the ONCD reporting on the progress and effectiveness of the strategy.

Viña then provided an update on other initiatives, including discussions that the ONCD is engaging in to encourage harmonization of cybersecurity examination standards and the ONCD/U.S. Department of the Treasury (Treasury Department's) continued study of the possibility of a cyber insurance federal backstop. Related to the federal backstop, Viña that the Treasury Department had issued a request for input in 2023 and is currently studying responses, including considering what a federal backstop would cover, whether it would be mandatory, and what would trigger the backstop. Viña noted that the Treasury Department will host a Spring Symposium to continue the discussion and study of the matter.

Regarding ransomware, Viña noted that the ONCD has observed that ransomware incidents have gotten less common but more severe, indicating that threat actors are "big game hunting," seeking larger payouts for their activities. Ultimately, he said that the ONCD wants ransoms to be a last resort to avoid encouraging continued activity by threat actors.

Lastly, Viña referred to the ongoing discussions regarding the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which may impact insurers depending on the final determination of who is considered to be critical infrastructure.

Amann transitioned to the question-and-answer portion of the discussion, which began with a question from Chou. Chou asked about consumer perspectives on the ONCD'sr activity and consumer awareness of their use of data, particularly with regard to automobile monitoring/use of consumer data, including how to communicate with consumers. Viña noted that the ONCD was not going to work on communication with consumers as other agencies would address that via their own rulemaking process.

Romero asked about the timeline for the backstop discussions. Viña said the Treasury Department responded that its conference in the spring is the next meaningful milestone and suggested the Working Group connect with Steven Seize (Treasury Department) for additional information.

Amann asked about the significance of legacy systems as a root cause for cybersecurity events and how to encourage better recognition of the security threat legacy systems can represent. Amann also suggested that better underwriting practices could encourage better risk hygiene to, in turn, prevent more security incidents from occurring. Viña acknowledged the importance of the legacy systems discussion and pointed to the ONCD's work encouraging long-term investments because, with legacy systems, manufacturer support has typically ended; thus, security updates are no longer available, leading to increasingly vulnerable infrastructure.

Viña also introduced Jeff Rob (ONCD) as a colleague who will engage in cyber insurance matters going forward.

2. Discussed Other Matters

Peterson provided a brief update, noting that now that the Cybersecurity Event Response Plan (CERP) has been adopted, the next discussion will be about taking cyber event notifications safely and securely.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_Summer/WG-Cybersecurity/Minutes-CyberWG032724.docx

Draft: 08/08/24

E-Commerce (H) Working Group
Virtual Meeting
July 18, 2024

The E-Commerce (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met July 18, 2024. The following Working Group members participated: Judith L. French, Co-Chair (OH); George Bradner (CT); Johanna Nagel (IA); Craig VanAalst (KS); Tom Travis (LA); Cynthia Amann (MO); Martin Swanson (NE); Colton Schulz (ND); Elizabeth Kelleher Dwyer and Matt Gendron (RI) and Haelly Pease (SD). Also participating was Shannel Logue (PA).

1. Adopted Its April 4 Minutes

The Working Group met April 4 and took the following actions: 1) adopted its Nov. 20, 2023, minutes; 2) discussed its 2024 work plan; 3) adopted the E-Commerce Modernization Guide; and 4) discussed its next steps.

Swanson made a motion, seconded by Travis, to adopt the Working Group's April 4 minutes (Attachment Four-A). The motion passed unanimously.

2. Heard a Presentation from Canopy Connect on Open Insurance

Tolga Tezel (Canopy Connect) explained that Canopy Connect is an infrastructure for consumer authorized insurance data. Tezel explained that Canopy Connect helps businesses verify insurance information within seconds. Tezel explained that insurance information is exchanged manually between insurance and the businesses that need the insurance information and that Canopy Connect provides ways to modernize and expedite this information transfer.

Tezel provided an overview of traditional intake methods that companies use to gather consumer data. Those methods are forms, interrogation, prefill, and declarations pages. Tezel stated that it can take a consumer more than 30 minutes to fill out insurance forms and that there is an approximate 50% abandonment rate before a consumer receives a quote. Tezel explained that the interrogation process occurs when consumers are asked questions by insurance companies that they might not know the answer to, including questions like an insured's vehicle identification number (VIN), annual mileage, premiums, policy limits, and deductibles. Tezel explained that most consumers do not have this information readily available and might not know where to find this information. Tezel explained that Canopy Connect solves these issues.

Tezel stated that the way Canopy Connect's product works is similar to open banking. Canopy Connect provides businesses with a platform where insurance companies can send a consumer a link where the client can sign in, and the business receives the permissioned insurance data directly from the current carrier. This process takes about 20 seconds and makes it easier for the consumer to share their information with the business of their choosing. Tezel explained that more than 1 million insureds have taken control of the data using consumer-authorized infrastructure. Insurers that use Canopy Connect make it easier for consumers to share their information with their insurance company for the insurer to provide the customer with a competitive proposal and to educate the consumer on what products can better suit a customer's needs. Tezel stated that Canopy Connect can help mortgage lenders and other companies verify insurance for their employees or for consumers that that they are lending to.

Draft: 04/16/24

E-Commerce (H) Working Group
Virtual Meeting
April 4, 2024

The E-Commerce (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met April 4, 2024. The following Working Group members participated: Troy Downing, Co-Chair (MT); Judith L. French, Co-Chair (OH); Alex Romero (AK); Jully Pae (CA), George Bradner (CT); Craig VanAalst (KS); Chlora Lindley-Myers (MO); Martin Swanson (NE); Colton Shulz (ND); Travis Jordan (SD); and Charles Malone (WA).

1. Considered Adoption of Its Nov. 20, 2023, Minutes

Director Lindley-Myers made a motion, seconded by Schulz, to adopt the Working Group's Nov. 20, 2023, minutes (*see NAIC Proceedings – Fall 2023, Innovation, Cybersecurity, and Technology (H) Committee, Attachment Four*). The motion passed unanimously.

2. Discussed its 2024 Work Plan

Director French stated that the Working Group met March 5 in regulator-to-regulator session to discuss its work plan for the year (Attachment Four-A1). Director French stated that the work plan includes adopting the E-Commerce Modernization (Guide) and then making appropriate amendments as the Working Group meets throughout the year.

3. Adopted the Guide

Director French explained that the Guide was exposed for a 20-day regulator-only comment period that ended Feb. 6. The necessary changes were made, and the Guide was then exposed for a 30-day public comment period that ended March 14. Director French further explained that NAIC staff received one comment from the Insured Retirement Institute (IRI). Director French asked if anyone from IRI wanted to make any comments.

Sarah Wood (IRI) stated that she appreciates the work the Working Group has completed thus far and that the current Guide is helpful and provides a good summary of the information gathered during the survey. She stated that IRI members are unsure how states will use the Guide going forward. Wood stated that she would be interested in hearing from anyone who might have insight on that issue.

Miguel Romero (NAIC) responded that the Guide is a starting point for any state looking to update its regulatory framework. Romero further stated that the Guide can assist new state insurance regulators in finding efficiencies in their regulatory processes and provide a good starting point for further research.

Schulz stated that he agreed with Miguel Romero's comments about the Guide being a starting point and that the Guide takes industry comments and categorizes them based on how easy or difficult a particular e-commerce topic could be to resolve. Wood responded that it was good to hear that the Guide is considered a first step.

Schulz made a motion, seconded by Alex Romero, to adopt the E-Commerce Modernization Guide (Attachment Four-A2). The motion passed unanimously.

4. Discussed its Next Steps

Director French explained that the Working Group will have another meeting to receive presentations. She said that NAIC staff are currently working on communicating with possible presenters and will send a meeting notice with further information once it is available.

Having no further business, the E-Commerce (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/Member Meetings/H CMTE/2024_Summer/WG-E-Commerce/2024 0404Interim-Meeting/Minutes/Minutes-E-CommerceWG042024.docx

Tezel then touched on Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) and the precedent it has set with open banking and how that precedent should apply to insurance. The Dodd-Frank Act provides that a consumer financial services provider must make available to a consumer information in the control or possession of the provider concerning the consumer financial product or service that the consumer obtained from the provider. Tezel explained that Section 1033 helped the financial services industry provide consumers with enhanced control over their financial lives.

Tezel explained that consumers are missing the right to authorize access to their insurance information and that state insurance regulators, through the NAIC, should create models to allow this. Tezel explained that all of the NAIC data privacy models are missing consumer-authorized data access. Tezel suggested that state insurance regulators should take the language from Section 1033 and include it in a NAIC data privacy model. Tezel explained that adding this language to a NAIC data privacy model will promote responsible innovation in insurance.

Gendron asked Tezel if he had submitted comment letters to the Privacy Protections (H) Working Group with the draft language from Section 1033. Tezel responded that Canopy Connect sent comments after the comment period closed. Therefore, it has not sent comments formally. Gendron responded that there should be another opportunity to provide comments on the selected privacy model. He said that he has used an open banking platform and noted that he might not have been aware that the platform was going to sell his information, but he saw value in this discussion, and he is looking forward to seeing if Section 1033 language could be added to the data privacy model.

Schulz commented that in 2021, there was a proposal to have language similar to Section 1033 to allow consumers to easily share their information, but the domestic insurers blocked the legislation. Schulz explained further that adding the proposed language could have some pushback because insurers think that allowing consumer-authorized access to data could increase competition. Tezel said that he has had discussions with a few state insurance departments, and the general takeaways are that: 1) state insurance departments expect the treatment of insurance to be similar to banking; and 2) most consumers want the choice to authorize key financial data about themselves.

Logue commented that open insurance has been popular in Brazil and the United Kingdom. Logue stated that she can see how insurance companies would not like this because open insurance allows consumers to find out if they can get better rates or other plans. She said she is curious to see how open insurance is received in the future. Logue asked if open insurance had been mentioned during the open comment period for Section 1033. Tezel responded that he is unaware of the Consumer Financial Protection Bureau (CFPB) exploring open insurance and that he wouldn't expect the CFPB to do so because insurance is regulated at the state level. Tezel said that in talking with major insurance carriers, the general response to open insurance is either positive or neutral. Tezel stated that the adoption of Section 1033 that made it possible for consumers to share their data and that innovated the banking industry.

Miguel Romero (NAIC) reiterated Logue's point that open insurance is discussed internationally, and he wondered why it has not been spoken about in the United States. Romero stated that he worked with E-Commerce (H) Working group leadership to set up this presentation, but he sees this conversation being moved to the Privacy Protections (H) Working Group, but he thought this would be a good setting for an educational discussion. Romero asked if any consumer representatives had an opinion on the discussion.

Birny Birnbaum (Center for Economic Justice—CEJ) stated that open insurance is something that consumer representatives support because it empowers consumers and promotes more competitive insurance markets. Birnbaum also said that there are simple guardrails for protecting consumers' data by simply stating that the aggregators of the consumer data should be prohibited from reselling the data.

Tezel responded and stated that Canopy Connect does not resell its customers' data, and that can be found in their privacy policy. Brendan Bridgeland (Center for Insurance Research—CIR) agreed with Birnbaum's comments and stated that consumers should be the owner of their data and that any other assumption is contrary to consumer interests. Bridgeland also added that similar language to Section 1033 should be added to the NAIC privacy model law.

Gendron responded to the consumer representative comments and stated that he is not sure that they could license data vendors in Rhode Island under its current statutes. Therefore, he does not know how states could enforce the prohibition of selling a consumer's data. Birnbaum responded stating that the NAIC is in the process of revising its privacy model law and that there is nothing in that model law or any model that limits a state from prohibiting a third party who collects data from selling the consumer's data. He said that just because data vendors are not licensed entities does not limit what state insurance regulators can do with the model law.

Schulz asked Tezel what kind of data Canopy Connect collects. Tezel responded that it collects consumer personal data that is connected with the products that they have purchased with their insurance provider. Norman Tan (Canopy Connect) added that the information that they receive is the information that is available on the declarations page like named insureds, premiums, policy limits, deductibles, and the effective dates of the policy. Tan further explained that a consumer could take their information from the declarations page of their insurance policy and share that, but Canopy Connect facilitates the transfer so that the information-sharing process is more secure.

Director Dwyer commented that this is a complicated issue and that it should be discussed in the Privacy Protections (H) Working Group. She followed up on Gendron's comment that when Rhode Island adopted the original NAIC privacy model law, Rhode Island adopted it as a regulation. Therefore, Rhode Island would have the authority from its legislature in order to prohibit a data vendor from reselling data.

3. Discussed its Next Steps

Director French said that the Working Group will have another meeting to receive presentations. She said that NAIC staff are currently working with Pennsylvania, which will present on its Key Smart Launch program.

Having no further business, the E-Commerce (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/Member Meetings/H CMTE/2024_Summer/WG-E-Commerce/2024 0718Interim-Meeting/Minutes/Minutes-E-CommerceWG071824.docx

Attachment Four-A1
Innovation, Cybersecurity, and Technology (H) Committee
8/15/24

2024 Adopted Charges and Workplan

E-Commerce (H) Working Group

Commissioner Troy Downing (MT), Co-Chair
Director Judith French (OH), Co-Chair

The **E-Commerce (H) Working Group** will:

A. Examine e-commerce laws and regulations to aid in identifying updates to the E-Commerce Modernization Guide.

The regulator only comment period ended on February 6, 2024. The open comment period ended on March 14, 2024.

Recommend:

- Expose the E-Commerce Modernization Guide for public comment after the regulator only comment period and adopt the Guide early in the year.
- Consider having a public meeting in March or April to discuss this proposed Workplan and adopt the Guide.
- Possibly adopt amendments as we meet with industry, regulator, and consumer representative to identify additions to the Guide.
- Explore the following topics:
  - Telemedicine
  - Rose of InsureTech
  - Telehealth
  - Privacy
  - EPayPolicy- a product designed for rapid routing, processing and reconciliation of paper check payments for the insurance industry.
  - Discuss Pennsylvania's electronic licensure process for insurance licensing forms.

B. This may include meeting with industry experts to understand industry trends that may impact laws and regulations

Possible Presentations Could Include:

- Sending an invitation to industry to see who would want to talk to the Working Group about the document and where the Working Group is headed.

- Sending an invitation to present to Pennsylvania and a representative from Canopy Connect, (a digital infrastructure that offers easy permissioned sharing to businesses looking to streamline gathering data from consumers), so that the Working Group can hear a presentation on open insurance to understand what the trend is and how the trend may might require additional modernization or revisions to the regulatory framework as well as add consideration of commercial liens and it could touch on producer/agent topics as well.
- Engage with industry and consumer representatives to consider additional topics for addition to the modernization guide.

SharePoint/Member Meetings/H Cmte/2024 Summer/WG-E-Commerce/2024 0404Interim-Meetings/Materials/E-Commerce Working Group 2024 Workplan 3-25-2024.docx

Draft: 4/4/2024

Adopted by the E-Commerce (H) Working Group, April 4, 2024

E-Commerce Modernization Guide

In 2021, the E-Commerce (H) Working Group sent a survey to the states asking what exceptions to state laws or regulations were implemented during the pandemic that allowed electronic commerce, electronic transactions, and electronic communications to take place when in-person methods were not possible. The survey also asked whether any of these exceptions had expired, had been rescinded or were made permanent either by legislation or through department action.

The Working Group also sent a survey to insurers and industry stakeholders asking them to identify any specific technologies, communications, transactions or any other forms and methods of electronic commerce that may currently impede their ability to conduct business electronically, in part because many of the exceptions to state law or regulation that were put in place during the pandemic may no longer be in effect.

After receiving and discussing the survey results, the Working Group organized the responses into a format best suited for consideration going forward. That format organizes the areas of concern into the following five broad categories: (1) e-signature; (2) e-notices; (3) policy issues; (4) claims; and (5) a general “other” category.

The purpose of this Guide is to memorialize the insights gained through that initial survey project and in subsequent engagement with industry representatives. Furthermore, this document hopes to advise regulators on e-commerce laws and regulations and provide uniform guidance on various e-commerce topics. When reviewing this Guide, please note that for opt-in/opt-out of electronic notifications and transactions, ERISA, UETA, and other relevant federal laws could preempt state laws in the life and health context.

Additional consideration may need to be given to the various contexts in which the regulatory requirements that follow are enacted. For instance, Departments using the guidance that follows may find it necessary to have differing requirements based on the type of consumer impacted (*i.e.*, individuals vs. businesses). Initially, this document was referred to as a framework, however, as the document has since evolved, it has been adopted as a guide.

(1) E-SIGNATURE

The first category is e-signature. The Uniform Electronic Transactions Act (UETA) defines electronic signature or e-signature as “an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.” The topics in the e-signature category are wet signatures, remote online notarizations (e-notary or RON), and elimination or minimization of notarization requirements.

Topic	Explanation of Topic	Industry Request	Concern With Industry Request	Possible Solutions	Possible Complications
Wet Signatures	A wet signature is created when an individual physically marks a document, as opposed to e-signature, which happens electronically	Allow affirmative opt-out for e-signatures, make opt-in the default	No conscious decision made for e-signature by consumer	Add opt-in clauses to applications and policies to allow for e-signatures and e-notices	Employee training; may require amending existing state laws; consent to e-signature limited to per transaction

The NAIC’s public comment process resulted in the following input:

- Overall, industry supports the use of e-signatures.
- The Center for Economic Justice (CEJ) does not believe opt-in should be the default due to the possibility that consumers could consent to terms and conditions that they might not be aware of.
- Northwestern Mutual suggested that concerns could be mitigated by ensuring the signer is provided access to the document during and following the e-signature event.

Topic	Explanation of Topic	Industry Request	Concern With Industry Request	Possible Solutions	Possible Complications
Remote Online Notarizations (E-Notary or RON)	A remote online notarization generally allows a signer to personally appear before the notary using audio-visual technology instead of being physically present in the same location as the notary	Remaining states should all adopt some form of RON	Could create doubt regarding signature authenticity	Issue bulletin(s) or change(s) in interpretation that RON meets notary requirements	Employee training; may require amending existing state laws; consent to e-signature limited to per transaction

The NAIC's public comment process resulted in the following input:

- The Center for Economic Justice suggests that such a change be paired with the condition that consumers are provided with clear disclosures regarding the safeguards and potential dangers of using RON.

Topic	Explanation of Topic	Industry Request	Concern With Industry Request	Possible Solutions	Possible Complications
Eliminate/Minimize Notarization Requirements	There is the potential to eliminate or minimize notarization requirements that may present unnecessary regulatory barriers	Statutory modifications and policy updates to clarify where notarization is still required	Notarizing signatures helps guarantee that the signature is authentic	Survey states asking whose statutes require notarization and why these are necessary	May require amending existing state laws; State legislature and/or Governor disagreeing with doing so

The NAIC's public comment process resulted in the following input:

- The CEJ emphasized the importance of specific guidelines for fraud detection and prevention to maintain the integrity of the notarization transaction and urged that consumers should be informed of these safeguards.

(2) E-NOTICES

The second category is e-notices. This category examines the electronic delivery of insurance documents, including the electronic delivery of notices (or e-notices). The topics in the e-notices category are wet signatures, lapse/termination notices, proof of delivery, and replacement questions (life insurance application).

The NAIC's public comment process resulted in general insight applicable to the discussion of E-Notices, broadly. The American Council for Life Insurers (ACLI) suggests Departments encourage consumers to proactively update e-mail addresses helping ensure consumers are timely updated on relevant matters from their insurers.

The NAIC's public comment process resulted in the following input:

- The CEJ does not believe opting in should be the default due to the possibility consumers could consent to terms and conditions of which they might not be aware.
- The ACLI notes that there may be benefits to e-signatures, asserting that with proper controls, it is much harder to alter an e-document that has been e-signed after signature (as there are typically audit logs registering every change, certificates of completion, or similar processes and controls in place). As a result, if someone alters a document after e-signature, it is detectable. Conversely, if a paper document is altered after wet signature, there may not be evidence to prove when the document was altered and whether the signer agreed to the alteration.

Topic	**Explanation of Topic**	**Industry Request**	**Concern With Industry Request**	**Possible Solutions**	**Possible Complications**
Wet Signatures	A wet signature is created when an individual physically marks a document, as opposed to e-signature which happens electronically	Allow affirmative opt-out for e-signatures, make opt-in the default	Many consumers still want applications, policies and correspondence on paper and will refuse opt-out	Amend UETA and/or insurance specific statutes, laws, rules, bulletins to allow a uniform, streamlined approach aligning state and federal laws related to e-signatures.	UETA much broader than just insurance; may require amending existing state laws

Topic	**Explanation of Topic**	**Industry Request**	**Concern With Industry Request**	**Possible Solutions**	**Possible Complications**
Lapse/Termination Notices	This topic focuses on the electronic delivery of lapse/termination notices to policyholders	Make electronic communication equal to First class mail; modify UETA and state laws allowing for delivery electronically	Many consumers still want applications, policies and correspondence on paper and will refuse opt-out	Bulletin, regulation or statute to allow for e-delivery any time communication must be sent if valid client email is known.	UETA much broader than just insurance; may require amending existing federal E-SIGN and state laws

The NAIC's public comment process resulted in the following input:

- The ACLI stated that it may be appropriate to consider adding disclosures that inform insureds that they must keep insurers informed of their contact information as all correspondence will be sent electronically.

Topic	**Explanation of Topic**	**Industry Request**	**Concern With Industry Request**	**Possible Solutions**	**Possible Complications**
Proof of Delivery	This topic focuses on how an insurer may demonstrate the successful electronic delivery of an insurance document	Allow for presumption of delivery if email is not returned as undeliverable	Property and casualty statutes in many states are different and require different notices	Bulletin, regulation or statute to allow for e-delivery any time communication must be sent.	May require amending existing state laws; State legislature and/or Governor disagreeing with doing so

The NAIC's public comment process resulted in the following input:

- The ACLI believes that there should be a presumption of delivery if email is not returned as undeliverable and that that notion should be universal.

Topic	**Explanation of Topic**	**Industry Request**	**Concern With Industry Request**	**Possible Solutions**	**Possible Complications**
Replacement Questions (Life)	If a policyholder is contemplating purchasing a life insurance policy or annuity contract and discontinuing or changing an existing policy or contract, Model #613 requires the applicant to initial if he or she does not want notice read aloud	Revise replacement model, allow replacement questions and disclosures to be part of a digital application process	Model #613 requires producer to leave the original or copy of all sales materials at time of application; also requires electronic sales materials be provided in printed form no later than time of policy/contract delivery	Do all states have the most up-to-date model? Or does industry want the entire model revised?	NAIC must compile which version of the model each state has adopted; possible that few states have adopted updated model with others not realizing their version is outdated

The NAIC's public comment process resulted in the following input:

- The CEJ emphasizes the need for consumer protection in the digital application process. They recommend that consumers receive access to the exact text of the questions and answers for their review and documentation. Additionally, they express concern about potential misrepresentation and misinterpretation of information involved in the replacement decision, making regulatory oversight of digital interfaces essential.
- The ACLI noted that there might be an issue with the effect on census enrolled cases when there is no actual enrollment event and no application.
- The Insured Retirement Institute (IRI) supports modernization of model regulations for annuity-related disclosures and notices but believes that replacement questions could be addressed through a Model Bulletin or Guidance instead.

(3) POLICIES

The third category is policies. This category focuses on the insurance policy. The topics in this category are state variations in policy requirements, regulations that include content or filing requirements of enrollment forms, re-delivery requirement of replacement notices in paper form if initially provided electronically, enrollment in employer group coverage, and UETA exclusion of delivery of notices of cancellation or termination of life insurance benefits.

Topic	**Explanation of Topic**	**Industry Request**	**Concern With Industry Request**	**Possible Solutions**	**Possible Complications**
State Variations in Policy Requirements	The industry raised concerns that minor variations in insurance policy requirements limit its ability to do business online and require excessive expense to create unique code for each state	Make uniform requirements for issues such as replacement question language, fraud warnings and marketing disclosures that do not materially affect consumer protections		Encourage uniform adoption of NAIC model regulations	

The NAIC's public comment process resulted in the following input:

- Overall, industry supports the use of uniform policy requirements that would not limit its ability to do business online.
- The CEJ supports uniform disclosure requirements, but only if they include substantial and effective consumer protections.

Topic	**Explanation of Topic**	**Industry Request**	**Concern With Industry Request**	**Possible Solutions**	**Possible Complications**
Regulations that include content or filing requirements of enrollment forms	The industry raised this topic particularly as it relates to enrollment in employer group insurance coverages	Forms or applications may each have different legal requirements depending on the type of policy and/or state; need uniformity		Each electronic application must be approved prior to use by the Department; all changes must be approved	

The NAIC'S public comment process resulted in the following input:

- The CEJ suggests that the lack of enrollment form uniformity among the states should not be a high priority for the E-Commerce Working Group.

Topic	**Explanation of Topic**	**Industry Request**	**Concern With Industry Request**	**Possible Solutions**	**Possible Complications**
Re-delivery requirement of replacement notices in paper form if initially provided electronically	The industry raised concerns that some states require delivery of the replacement notice in paper form for life and annuity sales	This unnecessarily duplicates the effort required by the insurer; eliminate any state law requirement that requires paper delivery			May require amending existing state laws; consumers would have to affirmatively opt-out of electronic communications

Topic	**Explanation of Topic**	**Industry Request**	**Concern With Industry Request**	**Possible Solutions**	**Possible Complications**
Enrollment in Employer Group Coverage	This topics centers on enrollment in employer group coverages, particularly as it relates to various employer policyholder and/or vendor electronic enrollment platforms		Product filings can be very complex; different state disclosure, signature or delivery requirements; age-based requirements		Complexity of filings; forms within a policy or contract may differ on what can/cannot be shared electronically; e-delivery requirements are difficult to implement due to state variations

The NAIC's public comment process resulted in the following input:

- The ACLI stated that policy delivery to an employer/group policyholders should be streamlined in terms of e-delivery and e-consent.

Topic	Explanation of Topic	Industry Request	Concern With Industry Request	Possible Solutions	Possible Complications
UETA excludes delivery of notices of cancellation or termination of life insurance benefits	Similar to the lapse/termination notices topic in the e-notices category above, this topic focuses on the electronic delivery of notices of cancellation or termination of life insurance benefits	Identify which states still have these requirements; amend state law to remove exclusion			

The NAIC's public comment process resulted in the following input:

- The IRI supports e-delivery of documents as the default option, allowing consumers to opt-out of e-delivery if they prefer paper documents. They believe that this approach is aligned with increasing consumer expectations for electronic transactions and provides the tools regulators and insurers need in order to identify and deter fraud.
- The IRI expresses concern about the proposed differentiation between e-insurers and paper insurers, which may create unnecessary complexity and potential impediments to uniform modernization. They also stress that differentiation could provide some insurers with an unfair competitive advantage or cause confusion among consumers.

(4) CLAIMS

The fourth category is claims. This category focuses on insurance claims. The topics in the claims category are claims processing and minimize/modernize licensing requirements related to claims adjustment.

Topic	Explanation of Topic	Industry Request	Concern With Industry Request	Possible Solutions	Possible Complications
Claims Processing	After a policyholder reports a loss, the use of drones may help expedite the processing of the insurance claim	Allow for the use of drones		Express statutory or regulatory authority for the use of such technology	Concern for accuracy

The NAIC's public comment process resulted in the following input:

- The CEJ expressed concerns about the use of drones for claims processing, citing data privacy and digital rights issues. They believe insurers should obtain upfront consent from consumers for the use of data and include drone use provisions in policy forms, which would allow regulators to review and approve the terms of such use.
- The CEJ emphasized the need for clear guidelines and guardrails to ensure that the use of drones does not result in unfair terms or practices.

Topic	Explanation of Topic	Industry Request	Concern With Industry Request	Possible Solutions	Possible Complications
Minimize/Modernize licensing requirements related to claims adjustment	The industry raised the potential opportunity to minimize/modernize licensing requirements related to claims adjustment.			Amend statutes to allow digital adjustment of claims; eliminate licensing requirements or provide option for a business license (as opposed to individual licenses); allow online licensing courses; allow fingerprints submitted in one state to be valid in all states for a set amount of time	

The NAIC's public comment process resulted in the following input:

- The ACLI strongly supports the proposed industry solutions to modernize licensing requirements related to claims adjustment including allowing online licensing courses, utilizing fingerprints across multiple jurisdictions, and providing additional licensing options. They believe that these changes would help support diversity, equity, and inclusion initiatives within both the NAIC and the life insurance industry.
- The CEJ expressed reservations about the proposal to eliminate licensing requirements for adjusters. They believe that licensing adjusters is important for a variety of reasons and question whether the E-Commerce Working Group is the appropriate forum for discussing adjuster licensing proposals.

(5) OTHER

The fifth category is other. This category focuses on other topics that did not fit into any of the four categories above. The topic in the other category is different design element requirements for forms/documents and online materials.

Topic	**Explanation of Topic**	**Industry Request**	**Concern With Industry Request**	**Possible Solutions**	**Possible Complications**
Different design element requirements for forms/documents and online materials	The industry raised concerns regarding the various requirements across the states for forms/documents and online materials.	Various requirements across the states are difficult to implement	Document design/website/font size/formatting rules differ	NAIC should work with states to seek uniform standards; standards would allow companies to follow well-defined rules and departments to enforce violations	

The NAIC's public comment process resulted in the following input:

- The ACLI supports the Guide's proposed solution for addressing different design element requirements for forms/documents and online materials. They also emphasize the need to avoid duplicating the efforts of other NAIC workstreams and encourage the working group to remain focused on the core issues hindering e-commerce modernization.

Draft Pending Adoption

Draft: 8/27/24

Technology, Innovation, and InsurTech (H) Working Group
Chicago, Illinois
August 13, 2024

The Technology, Innovation, and InsurTech (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met Aug. 13, 2024. The following Working Group members participated: Eric Dunning, Chair (NE); C.J. Metcalf, Co-Vice Chair (IL); Matt Walsh, Co-Vice Chair (OH); Lori K. Wing-Heier (AK); Mark Fowler (AL); Chris Erwin and Letty Hardee (AR); Lucy Jabourian (CA); George Bradner and Wanchin Chou (CT); Jason Lapham (CO); Karima M. Woods (DC); Tim Li (DE); Doug Ommen (IA); Dean L. Cameron and Weston Trexler (ID); Shawn Boggs (KY); Jackie Horigan (MA); Joy Y. Hatchette and Kory Boone (MD); Sandra Darby (ME); Chlora Lindley-Myers and Cynthia Amann (MO); Andy Case (MS); Brian Downs (OK); Mike Humphreys and Shanne Logue (PA); Colton Schulz (ND); Christian Citarella (NH); Cassie Brown and Mark Worman (TX); Eric Lowe (VA); Ned Gaines (WA); Erin K. Hunter (WV); and Bryan Stevens and Lela Ladd (WY). Also participating were: Remedio C. Mafnas (MP); Scott Kipper (NV); Adrienne A. Harris and Bhavna Agnihotri (NY); and Michael Wise (SC).

1. Adopted its Aug. 29, 2023, Minutes

Schulz made a motion, seconded by Commissioner Humphreys, to adopt the Working Group’s April 29, 2023, minutes (*see NAIC Proceedings – Fall 2023, Innovation, Cybersecurity, and Technology (H) Committee, Attachment Two*). The motion passed unanimously.

2. Heard a Presentation from McKinsey & Company on InsurTech Trends and Developments

Jason Ralph (McKinsey & Company) provided a presentation on InsurTech trends and developments. He noted that the insurance industry is stable and profitable, but it faces challenges in relevance and economic value compared to other industries. InsurTechs can play a role in reshaping profit pools, transforming customer expectations, and creating sustainable business models. There are four archetypes of InsurTechs: 1) headliners; 2) incumbents; 3) tech giants; and 4) lesser-knowns focused on back-office improvement.

Ralph said that InsurTechs primarily focus on marketing and distribution within the property/casualty (P/C) space. He said the insurance industry has struggled with reducing costs, but there is an opportunity for InsurTechs to simplify and automate processes. The InsurTech funding environment has changed, with a decline in venture capital investment, but there are still growth opportunities. InsurTechs can learn from big tech companies in terms of age, revenue growth, profitability, and market cap. InsurTechs can have a significant impact on sales, distribution, pricing, underwriting, claims, operations, customer service, and information technology (IT) through personalized marketing content, automation potential, and streamlining processes.

Horigan asked if the InsurTech business models that industry is seeing are sustainable given their pace of innovation. Ralph responded that technology companies have a proven track record of continually innovating and keeping the pace of innovation ongoing.

Logue asked what state insurance regulators need to do with third parties who are not necessarily insurance companies, particularly given their profit incentives and the customer lifetime value (CLTV) model, which focuses on the highest-price consumers. Ralph responded that understanding incentives and business models can help lead to beneficial discussion between regulators and companies.

Schulz commented that he was excited to hear the discussion about generative (AI) helping with code generation as it may help address the ongoing legacy system issue that state insurance regulators have previously discussed.

Director Cameron asked about the spread of risks and whether InsurTechs risk segregating risk at such a granular level and lose some of the intention of insurance. Ralph said that industry has historically held this challenge as important and that he was confident that it would continue to be a foremost consideration.

3. Heard a Presentation from the InsurTech Coalition on its Work

The InsurTech Coalition—which includes Clearcover, Lemonade, and Next Insurance—supports public policy that enables innovation, including fostering an environment in which innovation can thrive responsibly. Jennifer Crutchfield (Clearcover) noted that the InsurTech Coalition membership collectively writes in every state offering commercial and personal lines coverage in addition to life insurance products. Scott Fischer (Lemonade) said that the InsurTech Coalition is driving discussions around innovation and responsibility in insurance. The Coalition’s membership wants to help push the insurance industry to where state insurance regulators wish it to be. Rachel Jrade-Rice (NEXT Insurance) closed by expressing several key areas where regulators and tech-forward companies can collaborate: supporting emerging businesses, allowing new business methods, promoting market access, and supporting reasonable data privacy and security regulation.

Having no further business, the Technology, Innovation, and InsurTech (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Member Meetings/H CMTE/Summer_2024/WG_TII/Minutes-TIIWGWG081324.docx

Draft Pending Adoption

Draft: 8/28/24

Privacy Protections (H) Working Group
Chicago, Illinois
August 14, 2024

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Chicago, IL, Aug. 14, 2024. The following Working Group members participated: Amy L. Beard, Chair (IN); Erica Weyhenmeyer, Vice Chair (IL); Richard Fiore (AL); Lori K. Wing-Heier and Chelsy Maller (AK); Gio Espinosa and Catherine O'Neil (AZ); Damon Diederich and Jennifer Bender (CA); Doug Ommen and Johanna Nagel (IA); Robert Wake (ME): Van Dorsey (MD); Jeff Hayden (MI); T.J. Patton (MN); Cynthia Amann (MO); Martin Swanson (NE); Santana Edison (ND); Michael Humphreys and Gary Jones (PA); Patrick Smock (RI); Frank Marnell (SD); Katie Johnson (VA); Todd Dixon (WA); Lauren Van Buren, Timothy Cornelius, and Andrea Davenport (WI); and Bryan Stevens (WY). Also participating was Kevin Gaffney (VT).

1. Adopted its July 10 Minutes

Commissioner Beard said the Working Group met July 10. During its this meeting, the Working Group took the following action: 1) adopted its June 12 minutes and 2) discussed an approach for revising the *Privacy of Consumer Financial and Health Information Regulation* (#672).

The Working Group also met Aug. 5, in regulator-to-regulator session, pursuant to paragraph 8 (consideration of strategic planning issues) of the NAIC Policy Statement on Open Meetings, to discuss the Working Group's next steps.

Edison made a motion, seconded by Amann, to adopt the Working Group's July 10 (Attachment Six-A) minutes. The motion passed unanimously.

Beard provided a brief recap of the work done since the Spring National Meeting when the Working Group reformed. She said the Working Group held an open meeting in May, where a privacy expert from Husch Blackwell presented on federal and state privacy legislation, and the Working Group received the industry's draft, which uses Model #672 as a framework. She said public comments were requested and received on whether to continue work on the new Model #674 or to revise an existing NAIC privacy model while taking into consideration the option of utilizing the revised Model #672 provided by the industry.

During the Working Group's June 12 open call, Commissioner Beard said the Working Group heard from members, interested regulators, and interested parties; discussed their comments; and voted to move forward with revising Model #672. On July 9, Beard said Working Group leadership met with 20 NAIC Consumer Representatives to hear comments specific to consumer needs. She said the call was productive and provided insight into the issues that are most important to consumers. Beard said that during the July 10 open call, the importance of transparency throughout the process was emphasized, and leadership noted that regardless of the framework used, the discussion around core privacy principles and protections would be open and collaborative.

2. Heard an Update on Federal Privacy Legislation

Shana Oppenheim (NAIC) said the American Privacy Rights Act of 2024 (APRA) would establish national consumer data privacy rights and set standards for data security. The bill also would require covered entities to be transparent about how they use consumer data and give consumers the right to access, correct, delete, and export their data, as well as opt out of targeted advertising and data transfers. The measure would set standards for data minimization that would allow companies to collect and use data only for necessary and limited purposes and prohibit the transfer of sensitive covered data to third parties without the consumer's affirmative express consent. The Federal Trade Commission (FTC), state attorneys general, and consumers could enforce violations of APRA.

Oppenheim said the House Committee on Energy and Commerce released APRA in April 2024 by Chair Rep. Cathy McMorris Rodgers (R-WA) and Senate Commerce Committee Chair Sen. Maria Cantwell (D-WA). She said an updated version of the bill was released 36 hours before the markup in late June and was abruptly canceled five minutes before the meeting after heavy pushback from top GOP leadership, tech lobbyists, and privacy advocates. She said no markup had been rescheduled so it was too early to know the timeline before the August recess and fall elections.

Oppenheim said some of the groups against it include: 1) law enforcement groups, which say giving individuals the right to request the deletion of their data from brokers could rob law enforcement of access to "common investigative research services and other investigative tools that are used successfully every day by local, state, and federal law enforcement agencies;" 2) the Interactive Advertising Bureau (IAB), representing 700 media companies, which said a) opt-in for sensitive covered data (ordinary browsing history) would be bad for targeted advertising, b) the exemption for small businesses was not practical because most of them use third-party online advertising to grow, c) preemption was not complete enough, and d) a private right of action would be bad; 3) United for Privacy, which said more preemption is necessary to create a uniform national privacy standard; 4) the Main Street Privacy Coalition (made up of 20 national trade associations), which is concerned with customer loyalty programs, common branding, and private right of action that would equate to a trial lawyer bonanza.

Oppenheim said APRA would apply to companies subject to the FTC Act, and even goes a step farther to reach nonprofit entities (covered entities). She said some small businesses (under $40 million in revenue and processing covered data of less than 200,000 individuals) would be exempt unless they generate revenue from sharing covered data with third parties. The APRA would cover all individuals and treat information about minors (defined as individuals under the age of 17) as sensitive covered data.

She also said covered data includes information that identifies or is linked or linkable to an individual or a device that is linked or linkable to one or more individuals. Oppenheim said this broad definition does not include de-identified data, employee information, publicly available information, inferences made exclusively from multiple independent sources of publicly available information (with certain conditions), or information in collecting a library, archive, or museum. She said sensitive covered data includes the same categories in state privacy laws, such as information revealing race, ethnicity, national origin, sex, government-issued identifiers (e.g., a social security number or driver's license number), information that describes an individual's past, present, and future health conditions and treatments, genetic information, financial account information, biometric information, or precise geolocation information. Oppenheim said the APRA considers private communications, account or device log-in credentials, information revealing sexual behavior, information regarding minors, images and recordings intended for private use or depicting the naked or undergarment-clad private area of an individual, an individual's viewing log video programming, information revealing an individual's online activities across websites, and other information the FTC determines to be sensitive covered data.

Oppenheim said the APRA requires covered entities to provide consumers with rights about their covered data and how it may be processed. She said these rights include the right to access their covered data, the correction of their covered data, the deletion of their covered data, and the right to the portability of their covered data. Oppenheim said covered entities must have flexibility and agility in their data storage practices, allowing for deletion or correction and providing portability. For example, if an individual requests a copy of all their covered data collected, the covered data can be exported in an accessible manner to be shared with the individual. These rights apply even if that data is going to be shared with a competitor or made public (except for derived data if it would result in the release of trade secrets or other proprietary or confidential data). Oppenheim said the APRA allows consumers to opt out of covered data processing and covered data use, including opting out of targeted advertising, algorithmic decision-making, and covered data transfers. She said the opt-out process should be straightforward and transparent. Oppenheim said the APRA further directs the FTC to establish requirements and technical specifications for a centralized mechanism for opt-outs within two years of the APRA's enactment.

She said the previous version included that for covered entities using algorithmic decision-making, and the APRA requires a clear and conspicuous notice to individuals that provides meaningful information on how the algorithm makes or facilitates a consequential decision—i.e., decisions that affect an individual's housing, employment, education enrollment, health care, insurance, or credit opportunities. Oppenheim said the APRA emphasizes that covered data should be restricted to specific, expected uses. She said this mirrors the language used in the General Data Protection Regulation (GDPR) of the European Union (EU) regarding data minimization and requiring a clear purpose for data collection. Oppenheim said covered entities and their service providers should closely examine their data collection practices and avoid the "collect-everything-we-can-and-sort-it-out-later" mentality. All information collected and retained should have a clear, explicit, and specified purpose.

Oppenheim said covered entities with more than $250 million in revenue and that collect large amounts of covered data or sensitive covered data (large data holders) must conduct privacy impact assessments (PIAs), which evaluate the impact of proposed data processing on privacy, to consider the potential risks and benefits of data collection. She said the previous version said covered algorithms were a computational process that makes a decision or facilitates human decision-making by using covered data, are also subject to impact assessments, and large data holders are required to detail the steps taken to mitigate the risk of harm to the following: minors, housing, education, employment, health care, insurance, credit opportunities, public accommodations based on protected characteristics, or disparate impacts based on such characteristics or on political party affiliation. Additionally, it said these PIAs and covered algorithm impact assessments should be transparent and clearly articulated, with recommendations to manage, minimize, or eliminate privacy-related impacts on a community.

Oppenheim said covered entities and service providers are required to have one qualified employee to serve as a privacy or data security officer. She said large data holders would be required to have two officers—a privacy and a data security officer. The data security officer must be a designated, qualified employee who oversees the organization's data protection efforts and ensures compliance with the APRA's requirements regarding consumer privacy rights, data minimization, and cybersecurity measures. Oppenheim said large data holders that trigger this requirement would be required to annually certify to the FTC their internal controls for APRA compliance and the reporting structure for the data security officer and other certifying officers, including the company's CEO.

Oppenheim said the APRA would permit individuals to sue with a private right of action for violations of the APRA. She said the legislation would not allow for mandatory arbitration clauses if the case involves minors, substantial privacy harm ($10,000), or specific physical or mental harm. She also said an individual may seek actual damages, injunctive relief, declaratory relief, reasonable attorneys' fees, and litigation costs. Oppenheim said this provision could lead to class action lawsuits and is very controversial. She said in addition to individuals, the FTC or state attorney generals may also enforce the APRA. Oppenheim said non-sectoral state privacy laws are preempted by the APRA, which means laws that address specific subsections of privacy rights, including employment, education, breach notifications, banking, health, and other narrow laws, are not preempted, but privacy laws that generally address all categories of personal data and all rights to the data as provided in the APRA will be superseded by the APRA. She said this can help to simplify the U.S. data privacy framework, but not all state regulators are happy with this idea based on the APRA having broader or narrower protections in comparison to their own laws.

Oppenheim said new sections in APRA 2.0 include a new section on the Children's Online Privacy Protection Act (COPPA 2.0) under Title II, which differs to a certain degree from the COPPA 2.0 proposal currently before the Senate (e.g., removal of the revised "actual knowledge" standard and removal of applicability to teens over age 12 and under age 17). She said the revised APRA draft includes a new dedicated section on privacy by design that requires covered entities, service providers, and third parties to establish, implement, and maintain reasonable policies, practices, and procedures that identify, assess, and mitigate privacy risks related to their products and services during the design, development, and implementation stages, including risks to covered minors.

Oppenheim said as an exception to the general data minimization obligation, the revised APRA draft adds another permissible purpose for processing data for public or peer-reviewed scientific, historical, or statistical research projects. She said these research projects must be in the public interest and comply with all relevant laws and regulations. If the research involves transferring sensitive covered data, she said the revised APRA draft requires the affirmative express consent of the affected individuals. Oppenheim said the revised APRA draft expands obligations for data brokers by requiring them to include a mechanism for individuals to submit a "delete my data" request. She said this mechanism is like the California Delete Act in that it requires data brokers to delete all covered data related to an individual that they did not collect directly from that individual if the individual so requests. While the initial APRA draft required large data holders to conduct and report a covered algorithmic impact assessment to the FTC, if they used a covered algorithm posing a consequential risk of harm to individuals, the revised APRA requires such impact assessments for covered algorithms to make a "consequential decision." She said the revised draft also allows large data holders to use certified independent auditors to conduct the impact assessments, directs the reporting mechanism to the National Institute of Standards and Technology (NIST) instead of the FTC, and expands requirements related to algorithm design evaluations. Oppenheim said while the initial APRA draft allowed individuals to invoke an opt-out right against covered entities' use of a covered algorithm to make or facilitate a consequential decision, the revised draft now also allows individuals to request that consequential decisions be made by a human. Oppenheim said the revised APRA draft's definition section includes new terms, such as "contextual advertising" and "first-party advertising." She said the revised APRA draft also redefines certain terms, including "covered algorithm," "sensitive covered data," "small business," and "targeted advertising."

Because the act is intended to establish a uniform national data privacy and data security standard, Oppenheim said it would preempt state law. However, she said the act also enumerates extensive exceptions that would preserve provisions of state laws related to employee privacy, student privacy, data breach notifications, and health privacy. Oppenheim said the APRA would also preserve several rights to statutory damages under state law. For example, in civil actions brought for violations related to biometric and genetic information in Illinois, the act would preserve relief set forth in the Illinois Biometric Information Privacy Act (BIPA) and Genetic Information Privacy Act (GIPA). Oppenheim said the act would also preserve statutory damages for security breaches under the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA). She said these rights would be preserved as the statutes read on Jan. 1, 2024. Like the American Data Privacy and Protection Act (ADPPA), she also said APRA would preempt comprehensive state data privacy laws, except for an enumerated list of current state laws, including consumer protection laws of general applicability and laws addressing employee privacy, student privacy, and data breach notification. Oppenheim said APRA would also broadly exempt "any data subject to" and in compliance with the requirements of Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) (GLBA); however, APRA does not specify whether state GLBA laws would likewise be preempted. As a result, for some entities, she said APRA may create a new layer of compliance requirements, requiring those entities already subject to state-implemented GLBA privacy regimes to also be subject to oversight by the FTC.

3. Heard a Presentation from Consumers’ Checkbook on Legacy Systems and the Protection of Consumers’ Privacy

Eric Ellsworth (Consumers’ Checkbook) said he is the director of health data strategy and that he has 25 years of experience in data science and software/IT management. As such, he developed, deployed, and decommissioned IT systems under privacy regulations. As the Health Insurance Portability and Accountability Act of 1996 (HIPAA) chief security officer in a clinical laboratory, he created and oversaw the organization’s HIPAA program. Ellsworth said he advocates for transparency and simplification of the consumer experience. He said insurers are at considerable risk of data breaches because they are high-value targets with lots of data and money. According to the 2022 Black Kite Cyber Insurance Report, more than 50% of the largest insurance carriers are three times more likely to experience breaches than the best-protected organizations. Ellsworth said potential losses and disruptions include an average ransomware cost of $4.65 million; regulatory fines; customer lawsuits; operational paralysis of 22 days for ransomware, which typically takes longer to fix and restore systems; premium increases to pay for company costs; and damage to the company’s brand. He said insurer insolvency can damage entire markets as one company’s practices can affect customers of many other companies.

Ellsworth said data privacy and cybersecurity are different but linked. He said cybersecurity means protecting information assets from intrusion. It is like having a fence, guards, and alarms around a warehouse. These items do not control what goods are stored or where they are shipped. He said data privacy is putting controls on how data is stored, used, and transmitted. He said deletion requests mean “to destroy all items from supplier A,” while opt-out means“don’t send supplier B’s gray pants to Canada.” Ellsworth said a company can have sufficient cybersecurity measures but no control over data flows, but that protecting consumers’ privacy requires both. He said consumer privacy rights require controlling data flows, which answers where a consumer’s data is stored, where it is being sent, and when a consumer exercises these rights, how the company will find their data and fulfill the request. This leads to legacy systems and legacy data. He said legacy systems are software that is outdated but still operational. It is no longer actively being maintained, upgraded, or supported, and there is no personnel with active knowledge of how the system works or what is in it. Many are still used for core business functions and often serve as only a way to access old records.

Ellsworth said legacy data is data that is stored in old systems via email, spreadsheets, hard drives, old servers, or with third-party providers. He said it is a default state of affairs where nobody has a full picture of what or where the data is. He said legacy systems are highly vulnerable and pose ever-increasing challenges to meeting privacy and security requirements. Ellsworth said delays in fixing or replacing legacy systems would increase costs, be more time-consuming, provide less support, be harder to find talent, and make purchasing cyber insurance difficult or more expensive. He said regulators and insurers should be accounting for costs and risks around legacy systems regardless of whether insurers can replace them now.

Ellsworth said insurers may not be able to get rid of all legacy systems, but they need to put into place organizational controls typically required to obtain cyber insurance to ensure that they collect, store, and use data in ways that protect privacy and ensure the ability to delete, modify, and account for data upon request. He said examples of control processes are maintaining inventory of which systems contain which data; training on how data can and cannot be used; approving IT systems and storage for sensitive consumer data (e.g., “secure folders”); and requiring approvals for new uses or transmissions of data. He said legacy systems can be assessed for risks, costs to keep and replace, and effects on consumers’ rights to delete or opt out of data sharing within these organizational controls. Ellsworth said HIPAA is America’s earliest and most broadly implemented privacy law with many of its conceptual parallels to the current model and in the CCPA. He said adopting HIPAA took work but was doable. Ellsworth said covered entities became accountable for safeguarding private information both in their own organizations and when sharing with third parties (business associates) and underwent organizational process and culture changes to bring control to their collection, use, and sharing of data. He also said health insurers were not bankrupted. Now, health insurers are rightfully concerned about uncontrolled disclosures and are upset by federal rules permitting app developers to access data without a business associate agreement.

Ellsworth said his recommendations for organizational controls are that: 1) the model law explicitly requires insurers to institute organizational controls around the collection, storage, and use of data with executive or board-level accountability mechanisms; 2) regulatory oversight of these processes use a risk-based model to allow insurers latitude while ensuring protection of consumers’ privacy with legacy system risks being addressed within these assessments, and financial risks arising from legacy system vulnerabilities be considered; and 3) regulators leverage other work in assessing quality of insurers’ privacy and security controls, such as cyber insurance assessments, HIPAA, and/or CCPA controls and documentation.

He said his recommendations for third-party service providers are that: 1) the model law imposes requirements on insurers in diligence and contracting with third parties; 2) obligates insurers to assess the capability of the third party to comply with contractual terms required under this model law; and 3) requires insurers to control and audit their accounts and set up with third-party service providers.

Ellsworth said his recommendations for timelines for deletions and modifications are that: 1) when a consumer requests deletion or modification of data, that data be deleted or de-identified within 45 days of receipt of request, and if additional time is needed, allow 45 more days to delete, provided the licensee explains to their state regulator why additional time is needed and the consumer is notified; and 2) state privacy laws setting these timelines mimic those in California, Colorado, Connecticut, Utah, or Virginia. He said additional recommendations are that: 1) if licensees demonstrate that full deletion is not possible, licensees should make best efforts to restrict access to and use of the data on legacy systems by masking or encrypting data so it is not readable; putting strict access controls in place so data is not accessible for use; and creating a “restriction list” to flag data that should not be used, even if is not deleted; and 2) apply administrative sanctions or financial penalties, where licensees do not show good faith efforts to comply.

4. Discussed its Next Steps

Commissioner Beard reminded the Working Group that its charges for 2024 are to update Model #672 in a transparent manner that is feasible and adaptable so states can implement it. She said a chair draft revising Model #672 was distributed to Working Group members and interested regulators for their review in advance of the Summer National Meeting. She said the chair draft is intended to serve as a starting place for the drafting group to begin their work, and it is not designed to represent any agreement or position of the Working Group. Beard said the chair draft includes pertinent information and principles pulled from the *NAIC Insurance Information and Privacy Protection Model Act* (#670), draft Model #672 Plus, draft Model #674, and state comprehensive privacy laws. She also said the chair draft focuses on four key privacy principles and believes the language and principles will be familiar to everyone from previous drafts and conversations: third-party arrangements; right to access, correct and delete; sale of personal information; and handling of sensitive personal information. Once again, Beard said she wanted to stress that the chair draft is meant to be a starting point for discussion, and none of the language has been finalized, so comments and discussion are welcomed and encouraged, as the group looks forward to seeing how the draft evolves to create consensus among Working Group members, interested regulators, and interested parties.

Commissioner Beard said the chair draft would be exposed to the public for a 30-day comment period following the Summer National Meeting. She said Lois Alexander (NAIC) would include an invitation for drafting group volunteers and guidelines for drafting group participation in the exposure draft email. Commissioner Beard said Weyhenmeyer would lead the drafting group, which will be open to regulators and interested parties. She said the guidelines for drafting group participation are intended to set expectations for drafting group members and promote productive drafting conversations. She said the Working Group will continue to hold open and regulator-only sessions, as needed, to determine the best privacy regime and draft a model law that reflects that. She said the Working Group also wanted to ensure that everyone understands the next steps in this process and their respective roles and responsibilities. Beard said the Working Group wants to hear from all parties and encouraged their participation by submitting comments and redlines during public comment periods and engaging with the drafting group.

Weyhenmeyer said comments will be requested on third-party arrangements only during the first 30-day exposure period.

Harry Ting (Healthcare Consumer Advocate) said he submitted comments prior to the Summer National Meeting and asked if they could be distributed now. Commissioner Beard said the comments would be considered with the other comments received during the exposure period. Silvia Yee (Disability Rights, Education, & Defense Fund) said regulators are the heroes in the consumer data privacy arena, as they have the power and authority to help humanity or not. She also said she would be happy to help the Working Group in any way she can.

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

SharePoint/NAIC Support Staff Hub/Committees/H Cmte/ 2024 Summer/Privacy/Minutes/Minutes-PrivacyWG081424.docx

Draft: 8/28/24

Privacy Protections (H) Working Group
Virtual Meeting
July 10, 2024

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met July 10, 2024. The following Working Group members participated: Amy L. Beard, Chair, and Victoria Hastings (IN); Erica Weyhenmeyer, Vice Chair (IL); Sarah Bailey (AK); Richard Fiore (AL); Catherine O'Neil and Lori Dreaver Munn (AZ); Damon Diederich and Jennifer Bender (CA); Johanna Nagel and Jordan Esbrook (IA); Rasheda Chairs, Kelli Hudson, Kathryn Callahan, and Van Dorsey (MD); Stacy Bergendahl (ME); Jeff Hayden, Renee Campbell, Joseph Garcia, and Danielle Torres (MI); T.J. Patton (MN); Chlora Lindley-Myers, Cynthia Amann, and Jo LeDuc (MO); Santana Edison and Colton Schultz (ND); Teresa Green (OK); Martin Swanson and Connie Van Slyke (NE); Raven Collins (OR); Gary Jones, Richard Hendrickson, and Jodi Frantz (PA); Patrick Smock, Matt Gendron, and Raymond Santilli (RI); Lisa Harmon (SD); Scott A. White, Katie Johnson, and Garth Shipman (VA); Amy Teshera (WA); Timothy Cornelius, Lauren Van Buren, and Barbara Belling (WI). Also participating were Rebecca Smid and Anoush Brangaccio (FL); Tracy Biehn (NC); Matthew Walsh (OH); Tanji J. Northrup and Shelley Wiseman (UT); and Mary Block (VT).

1. Adopted its June 12 Minutes

Commissioner Beard said the Working Group met June 12 and took the following action: 1) adopted its May 15 minutes; 2) heard comments from interested parties on its path forward; and 3) adopted its plan to move forward with the existing *Privacy of Consumer Financial and Health Information Regulation* (#672).

Swanson made a motion, seconded by Amann, to adopt the Working Group's June 12 minutes (Attachment Six-A1). The motion passed unanimously.

2. Heard an Update on Federal Privacy Legislation

Commissioner Beard said that Shana Oppenheim's (NAIC) update on federal privacy legislation was postponed due to a meeting with the U.S. Department of the Treasury running over time. She said Oppenheim would give the update during the next Working Group meeting.

3. Discussed an Approach for Revising Model #672

Commissioner Beard said the goal of the Working Group discussion was to determine how the Working Group would move forward with revising Model #672. She said there were a couple of agendas, but she wanted to set the landscape by saying there would be no vote today because the meeting is to consider Model #672 and #672+. She emphasized that it is not necessarily the vehicle that is important but rather how the group wants to open this process up. It is more about the content and what protections the Working Group wants to implement in the model. That is why the Working Group is having so many calls and discussions. It is to ensure everyone has enough time to consider draft Model #672+.

She said the quick-look document, which compares core principles, and the drafting outlines breaking the model into groupings for efficient discussion were posted to the Working Group's website. The Working Group would pull pertinent information and principles from other NAIC privacy models, such as the *NAIC Insurance Information and Privacy Protection Model Act* (#670), state comprehensive privacy laws, and other resources emphasizing transparency and collaboration.

Weyhenmeyer asked for Working Group members to volunteer to join a subject matter expert (SME) drafting group. Commissioner Beard said to watch for an email from Lois Alexander (NAIC), as she would be reaching out to Working Group members to invite them to volunteer in the drafting process. Additional materials, information regarding next steps in the drafting group process, and additional correspondence would be distributed before the next meeting to outline the plan and its process.

Diederich asked if there would be a vote at the Summer National Meeting on whether to use Model #672 or Model #672+ as the starting point for drafting revisions or if the Working Group would be moving straight into the process, pursuing SME group meetings, and begin drafting on that basis. Commissioner Beard said the Working Group would be moving straight into the Working Group process and diving into what protections the Working Group thinks should be included in the revisions to Model #672, as was voted on during its last meeting, which will allow the Working Group to consider which Model #672+ protections to include in its path forward.

Dr. Harry Ting (Healthcare Consumer Advocate) said the NAIC consumer representatives wanted to comment on using Model #672 versus Model #672+ as the starting point for the revisions. Peter Kochenburger (Southern University Law Center) said the consumer representatives believed that starting with draft Model #672+, which is an industry draft, sends the wrong message. He said any draft used as an initial starting point sets the tone of the draft throughout the process, which is true in any document drafted. The choice of an initial draft structures the conversation and deviating from it going forward becomes harder. He said that, particularly for a consumer protection model, it is not a good image for regulators to start with the regulated entities' preferred language. Peter Kochenburger (Southern University Law Center) said he felt regulators would do a good job of balancing changes recommended by all stakeholders, but that he and other lawyers prefer to write the first draft as it reflects their goals most effectively.

Commissioner Beard emphasized that the Working Group voted on the last call to move forward with Model #672 and that draft Model #672+ is out there for consideration. She also emphasized that the vehicle does not matter as much as the content.

Dr. Ting said the consumer representatives hoped the Working Group would also look at the privacy principles shared with the Working Group and interested parties developed by the Working Group last year. He said the consumer representatives strongly support those principles and hoped those principles would be used in drafting the model. Dr. Ting asked that the Working Group first seek agreement on those principles or, if changes need to be made, at least recognize them in advance so the Working Group can produce language that is clear on whether these principles are being followed. He also said the consumer representatives suggested using exposure draft *Insurance Consumer Privacy Protection Model Law* (#674) as of 7/11/23, Version 1.2, as well as draft Model #672+ because some of the provisions in draft Model #674 that consumer representatives feel are important are not in Model #672 or Model #672+. Adverse underwriting decisions are needed to help consumers who do not understand why they are being turned down for certain insurance coverage. Commissioner Beard noted that with all comments considered, transparency and collaboration are at the heart of the process.

4. Discussed Other Matters

Commissioner Beard reminded attendees that the Working Group's next meeting would be at the Summer National Meeting in Chicago, IL, on Wednesday, Aug. 14, at 2:30 p.m.

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

SharePoint/NAIC Support Staff Hub/Committees/H Committee/Working Groups/Privacy/2024/Summer/July 10 Minutes/Minutes-PrivacyWG071024.docx

Draft: 7/8/24

Privacy Protections (H) Working Group
Virtual Meeting
June 12, 2024

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met June 12, 2024. The following Working Group members participated: Amy L. Beard, Chair (IN); Erica Weyhenmeyer, Vice Chair (IL); Chelsy Maller (AK); Richard Fiore (AL); Gio Espinosa, Catherine O'Neil, and Lori Munn (AZ); Damon Diederich and Jennifer Bender (CA); Kristin Fabian and Anthony Franchini (CT); Doug Ommen, Johanna Nagel, and Jordan Esbrook (IA); Van Dorsey and Katheryn Callahan (MD); Stacy Bergendahl, Robert Wake, and Sandra Darby (ME); Jeff Hayden, Chad Arnold, Renee Campbell, Joseph Garcia, Joe Keith, and Danielle Torres (MI); Cynthia Amann and Jo LeDuc (MO); Santana Edison and Colton Schultz (ND); Martin Swanson and Connie Van Slyke (NE); Raven Collins (OR); Gary Jones, Richard Hendrickson, and Jodi Frantz (PA); Patrick Smock, Matt Gendron, and Raymond Santilli (RI); Frank Marnell and Larry D. Deiter (SD); Katie Johnson and James Young (VA); Todd Dixon, John Haworth, and Amy Teshera (WA); Timothy Cornelius, Lauren Van Buren, and Barbara Belling (WI); and Bryan Stevens (WY). Also participating were Rebecca Smid (FL); Paula Shamburger (GA); Adam Flores and Ruth Stewart (IL); Victoria Hastings (IN); Ron Kreiter (KY); Tanji Northrup and Shelley Wiseman (UT); and Kevin Gaffney and Mary Block (VT).

1. Adopted its May 15 Minutes

Commissioner Beard said the Working Group met May 15 and took the following action: 1) adopted its 2023 Fall National Meeting minutes; 2) heard a presentation from Husch Blackwell on federal and state privacy legislative efforts; and 3) received an industry privacy draft.

Kreiter made a motion, seconded by Van Buren, to adopt the Working Group's May 15 minutes (Attachment Six-A1a). The motion passed unanimously.

2. Heard and Discussed Comments Received from Interested Parties on its Path Forward

Commissioner Beard said that at the end of its May 15 meeting, the Working Group received a draft update of the *Privacy of Consumer Financial and Health Information Regulation Model Regulation* (#672) from industry. She said this draft was distributed to Working Group members, state insurance regulators, and other interested parties immediately following the meeting. She said this draft was also posted to the Working Group's public web page along with a quick look tool prepared by NAIC legal staff comparing the new draft *Insurance Consumer Privacy Protection Model Law* (#674), *NAIC Insurance Information and Privacy Protection Model Act* (#670), Model #672, and the industry's update to Model #672. The industry draft and quick look tool were publicly exposed for a two-week comment period that ended May 30, requesting comments specific to whether the Working Group should continue drafting the new Model #674 or revise an existing model. Commissioner Beard had asked that all comments be submitted in writing and that comments refer only to the Working Group's path forward.

Commissioner Beard said Lois Alexander (NAIC) summarized and compiled the comments (Attachment Two), which were distributed and posted May 31. The compilation notes that the Working Group received 21 written comments. Commissioner Beard said the Working Group would like to give those who wanted to speak about their comments the opportunity to do so; however, she said that given the number of comments received, she asked that each speaker limit their comments to three minutes and focus on their key points aimed toward the path forward.

Marnell said South Dakota supports setting aside Model #674 and the Working Group taking up Model #672 as a starting point.

Swanson said Nebraska agreed with what Marnell said, and they reiterated that today.

Diederich said given the overarching movement in the privacy space and what the federal government is doing right now, he is concerned about departing from the draft the Working Group has been working on to develop an entirely new model law from a decades-old model just as it was nearing completion and already included many of the comments noted during the latest two-week comment period that ended May 30. He also said that updating the old Model #672 would be very laborious and time-consuming, which is why the previous Working Group had decided to draft a new model. Diederich said he felt this should be kept in mind and that the rest of the comments in his letters speak for themselves.

Cornelius said Wisconsin would support moving forward with revisions to the draft Model #672; however, there are concerns. He said the Working Group needs to figure out the scope, and if it is not going to be revising Model #674, then Wisconsin would support Model #672 because there appears to be a consensus for it, and the Working Group needs to start working on a draft.

Harry Ting (Healthcare Consumer Advocate) said he would like to make a few comments relevant to the decision before the Working Group. He said the Cambridge Dictionary defines privacy as an individual's right to keep personal matters and relationships secret. He said the task before the Working Group is to protect his privacy. Dr. Ting said that he is not protected under the current law. He said he is no longer able to respond to most emails, texts, or phone calls unless he recognizes the sender because every day, individuals with ill intent get ahold of his personal information and use it to find ways to steal his money. Dr. Ting said he needs that protection because companies are manipulating him to let them use his information for their own purposes, even though he does not understand exactly what they are collecting or how they will use it, and most make it exceedingly difficult for him to protect his personal information. He said there is one thing consumer representatives agree on, which is that asking consumers to read and understand privacy policies and then decide whether to opt out to protect their personal information is not protecting them.

Dr. Ting said the protection of personal data from those who should not have access to it and the ability of individuals to determine who can access their personal information is of the utmost importance. He said consumers cannot protect their personal data from those who should not have access to it, determine who can have access to it, nor respond because consumers are never given the opportunity to decide via an opt-in as so many companies and third parties utilize an opt-out privacy policy that allows them to find ways to sell personal data and steal money.

Dr. Ting said many of his fellow NAIC consumer representatives have also made it clear that having to read pages of tiny print in a privacy notice to implement an opt-out is exceedingly difficult, even for an experienced insurance consumer advocate like himself. Dr. Ting said that the current models are inadequate and that NAIC consumer representatives prefer the new Model #674. He said Model #672 provides only for opt-out, which is difficult for consumers to understand and puts the responsibility for data privacy on consumers as they must read through volumes of information and figure out complex wording to select that they do not want data shared or sold when access to desired information is denied. Dr. Ting said the new Model #674 requires an opt-in, which provides much better consumer protection by putting the responsibility on insurers and third parties to obtain consent from insurance consumers prior to selling or sharing the consumer's personal data. He also said Model #672 provides no protection after data has been shared, but the new Model #674 does. Dr. Ting recommended that the Working Group create a template for states to include in the new model as a consent notice that insurers would be required to use to obtain a consumer’s opt-in prior to selling or sharing the consumer’s data with affiliates or third-party providers. He said a sample template was included with the consumer representatives’ comments.

Ken Klein (California Western School of Law) said his comments align with Dr. Ting’s. He said many websites currently use pop-up privacy statements that require a consumer to accept the privacy terms or not be able to access the information needed, which is an example of opt-out being used as a default that serves the insurance industry's needs. Klein said the issue is where two interests are in conflict. One is a business interest, which is the opt-out that industry wants, and the other is the opt-in, which is in the privacy interest and is what consumers need. He said one cannot have it both ways, so the choice before the Working Group is which interest they will choose as the default. Klein asked the Working Group members to support the new Model #674 and its opt-in provision, which serves consumers and should be the default because consumers simply will not engage in opt-out; therefore, it is up to state insurance regulators to protect consumers’ privacy by requiring opt-in within the model itself.

Silvia Yee (Disability Rights Education and Defense Fund—DREDF) said she and many other consumer representatives who put their comments in the chat feature agreed with Dr. Ting and Klein when they asked that the Working Group support the new draft Model #674 already in progress because she supports opt-in as the best privacy policy. Yee stated that she has sometimes opened a privacy window and has tried to follow the steps to opt out of having her personal information shared and sold for marketing purposes to third-party providers. She said that as an educated person and attorney experienced in insurance and consumer privacy issues, even she finds it increasingly difficult, especially as she is getting older, to keep up with the hundreds of distinct types of privacy selections that consumers must navigate today. Yee said she suspects she is not alone in that experience. She said it is not easy to understand what a consumer needs to do to protect their privacy, and even if they want to partially protect their privacy or give up some of it, there is no nuanced way to do it. Yee said for industry members who believe consumers can be educated so they understand how to opt out, industry could use those training talents to educate consumers on how to opt in because it is good for consumers to understand. She said consumers would also like to understand why this group was working cooperatively to draft a new model with consumer privacy protection, then abruptly make a last-minute change to suggest something else.

Erica Eversman (Automotive Education & Policy Institute) said she had grave concerns about the privacy protections in the existing Model #672, especially in the automotive insurance industry, because auto repair shops require consumers in need of accident repairs to sign a privacy notice relinquishing personal data that indicates the auto shop network absolutely complies with the Gramm-Leach-Bliley Act (GLBA). She said consumers do not understand the privacy notification requirements and safeguards under the GLBA, which are not explained in the notice from auto shop providers. However, consumers who refuse to sign these notices are refused service by the auto repair shop. Eversman argued that unlike the health insurance industry, which has the Health Insurance Portability and Affordability Act of 1996 (HIPAA) with specific notices written in clear, understandable language that is required to be used by all health care providers in order to access consumers’ personal medical information, the existing privacy Model #672 does not provide the same level of protection; or any level of protection unless the consumer goes through the complex, confusing opt-out process, which varies greatly from company to company. Therefore, she said the new Model #674 provides a far better foundation for actual consumer protections, as it requires opt-in, which is essential to ensuring consumers of non-health insurance are at least as protected as health insurance consumers.

Commissioner Beard reminded participants that the Working Group is taking comments today regarding whether its focus should be on continuing to draft the new Model #674 or on revising the existing Model #672. She said there will be many opportunities for all parties to provide comments on specific privacy principles.

Randi Chapman (Blue Cross Blue Shield Association—BCBSA) said BCBSA is fully aligned with the joint industry comments submitted and fully supports moving forward with Model #672 with the so-called "Plus" concept that would include the added consumer protections as opposed to starting with a new model.

Wes Bissett (Independent Insurance Agents & Brokers of America—IIABA) said the group should have received a joint comment letter submitted by a dozen or so trade associations previously referenced by Chapman, which is in the meeting materials. He said the letter suggested starting from Model #672 as a universal framework for these privacy laws. Bissett said it was entirely natural for the NAIC to want to review its model recommendation, especially since 20 states have adopted state comprehensive privacy laws with an eye toward bolstering existing models in support of those individual state privacy laws. He said the joint industry group would support the Working Group revising the existing Model #672 because it has been implemented in every state and is ubiquitous, so it makes sense to start from there. Bissett said, as an analogy, that if we were to revise the Constitution, we would also consider amendments that are added to it. He said we do not urge states to ratify the Constitution but rather encourage them to write a new one. Bissett said that we add amendments wherever appropriate, which is what the IIABA suggests the Working Group should do here. He said, as we heard from David Stauss (Husch Blackwell) a few weeks ago, there are some common issues that states have focused on, such as consumer request rights, data minimalization, the role and treatment of third-party service providers, and how sensitive personal information is handled. Bissett said there are only a small handful of issues that can be addressed appropriately by adding those to Model #672 without throwing out the framework that all states have adopted. He said the BCBSA urges the Working Group to support revising Model #672 with whatever changes the Working Group adopts to include the issues in the comprehensive privacy laws already enacted by individual states that will ensure interstate consistency in the Working Group's final product.

Eric Ellsworth (Consumers' Checkbook) said he thinks Model #674 provides a much more robust framework. He said that if you look at the quick look document in the meeting materials, it starts by asserting several rights that Model #672 does not have. Ellsworth said there was a lengthy process in drafting Model #674 of discussing why those rights are important to consumers, so going back to Model #672 is fundamentally about restarting that debate. He said he did not see any reason other than a technicality that has changed that debate in terms of why consumers need these protections. Ellsworth said that, as other consumer representatives had referenced, there have been ever-increasing cybersecurity, and data use reasons that have indicated the need for these protections as a foundation for the law. He said the other thing he wanted to point out is that, in practice, some of the debates came down to what degree insurers might have to be responsible for the actions of third parties, which is a foundational requirement he believes is not addressed in Model #672. Ellsworth said the other item is the type of protections available under HIPAA, which were the subject of debates and a point of critical contention for Model #674 as well, and that he did not see any reason why those debates should just be abandoned when they were just getting to the fundamental issues of protecting consumers in favor of going back to a weaker law.

Bonnie Burns (Consultant to Consumer Groups) said she supports the comments of all the other consumer representatives and the arduous work that had gone into drafting Model #674 and supports continuing work on that document.

Chris Petersen (Coalition of Health Carriers—Coalition) said the Coalition supports Model #672 as the vehicle because it has been adopted in all states and would serve as a base and foundation for state legislatures as they attempt to adopt it. He also said it reflects some of the Coalition's key principles, such as its belief that there needs to be a HIPAA safe harbor going forward in any model and that any fixes need to be well thought out. Petersen said the group believes Model #672 is working, so if changes are needed, they should be made from it. He said a lot of the issues being discussed today are not privacy issues and are not issues that insurance licensees can address. Petersen said hacking and cybersecurity are not privacy issues. He said if one clicks on a website and it is not an insurance licensee's website, it is not a department of insurance (DOI) issue; therefore, the DOI has no authority over it. Petersen said some arguments are being made for a comprehensive privacy law, but they are not arguments for an insurance privacy law. He said the Working Group needs to stay focused on the issue, which started when industry asked for a gap analysis to determine what the state insurance privacy issues are that DOIs can do something about. Petersen said it is too late to do that now, but if the Working Group keeps that in mind, they will realize that Model #672 is the preferred option.

Michael DeLong (Consumer Federation of America—CFA) said he echoed the comments of the other consumer representatives who said that Model #674 does a better job of protecting consumer privacy in that an opt-in consent for people to collect their information is better. He also said he would like to emphasize that a lot of times, people talk about the importance of consumer education when, in fact, they are trying to find a way to push the burden of privacy protection onto consumers rather than to protect consumers' privacy and safeguard their data.

Kristin Abbott (American Property Casualty Insurance Association—APCIA) said that, as others have mentioned, in the industry letter that APCIA submitted with 12 other organizations, she recommended that the Working Group revise Model #672. She said the organizations are eager to work with state insurance regulators and other interested parties to address the concerns being raised and how they can be incorporated into the Model #672 framework.

Amy Killelea (Consumer Advocate) said she supports all the other consumer representatives' points. In addition, she said she strongly believes that Model #674 is the best option. She also noted that the process itself is concerning and that the foundation of producing a protective law or model through an independent process does support the development of the new Model #674.

Cate Paolino (National Association of Mutual Insurance Companies—NAMIC) said one point that has not been made yet is what the implementation process would look like if Model #672 and Model #674 both existed in some states. She said it would require quite different platforms and questions about definitions and cause massive confusion from a compliance perspective. Paolino said building on that and clearly differentiating from the baseline of Model #672 would allow for less disruption and easier rollout from a compliance perspective, as companies are working to remain in compliance in states that have Model #672 through the process of the states that may choose to enhance with additional components that might be in Model #672 Plus.

Weyhenmeyer said the Working Group found itself in a spot last year where many of the members felt like Model #674 was not something that would be easily adopted in their states. She said that since that is the point of a model, members wanted to make sure it would be something that could be signed onto and adopted in most states, as well as be consistent with not only what is needed in the marketplace but also protect consumers. Weyhenmeyer said regardless of the direction the Working Group goes in, comments will be taken into consideration. She said the Working Group just wants to ensure that whatever is in place can be implemented in all states.

3. Adopted its Plan to Move Forward with the Existing Model #672

Commissioner Beard said the Working Group had reviewed all the comments, heard from those who wished to present, and considered additional questions and discussions as a group during this meeting. She said it appeared the majority agreed that the path forward should be to revise the existing Model #672; therefore, it was time for the Working Group to consider adoption of the path forward.

Marnell made a motion to revise Model #672.

Diederich called a point of order. He said the agenda did not indicate that the Working Group would conduct a vote during this call and wondered if the Working Group could proceed without it being scheduled. Weyhenmeyer said the third agenda item was “Consider Adoption of its Path Forward by Roll Call Vote.” Diederich said the agenda attached to the meeting invite did not include this item. Weyhenmeyer said the agenda posted to the public website and call calendar included the vote as the third item. Diederich said the May 15 version did not have this item. Alexander said the revised version posted to the public website June 5 did include the roll call item. Diederich retracted the point of order.

Marnell made a motion, seconded by Stevens, that the Working Group set aside the new Model #674, take up Model #672 as the basis for the updated model, and begin work on it as quickly as possible.

Commissioner Beard said the Working Group should do a roll call vote for the sake of transparency and clarity. Alexander called and recorded the vote.

The motion passed by roll call vote, with seven yeses (Iowa, Illinois, Nebraska, North Dakota, Rhode Island, South Dakota, and Wyoming); three yeses, with Maine’s caveat that the wording changes promised will be made (Kentucky, Maine, and Wisconsin); six nays (Alaska, California, Maryland, Missouri, Virginia, and Washington); and three abstaining (Alaska, Michigan, and Pennsylvania).

Lucy Culp (Leukemia and Lymphoma Society—LLS) asked if the vote was to start with the existing Model #672 or the industry draft. Commissioner Beard said it was to move forward with Model #672.

Commissioner Beard said the motion passed, and the path forward will be to revise the existing Model #672.

Commissioner Beard reminded attendees that the Working Group’s next meeting would be in mid-July.

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

SharePoint/ NAIC Support Staff Hub/Committees/H Cmte/ 2024 Summer/Privacy/Minutes/Minutes-PrivacyWG061224.docx

Draft: 6/3/24

Privacy Protections (H) Working Group
Virtual Meeting
May 15, 2024

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met May 15, 2024. The following Working Group members participated: Amy L. Beard, Chair (IN); Erica Weyhenmeyer, Vice Chair (IL); Chelsy Maller (AK); Catherine O'Neil (AZ); Jennifer Bender (CA); Kristin Fabian (CT); Jordan Esbrook and Johanna Nagel (IA); Ron Kreiter (KY); Van Dorsey (MD); Stacy Bergendahl (ME); Jeff Hayden (MI); Cynthia Amann (MO); Santana Edison (ND); Martin Swanson (NE); Teresa Green (OK); Raven Collins (OR); Gary Jones and Richard Hendrickson (PA); Patrick Smock (RI); Frank Marnell (SD); Katie Johnson (VA); John Haworth and Amy Teshera (WA); and Bryan Stevens (WY).

1. Adopted its 2023 Fall National Meeting Minutes

Beard said the Working Group met March 8 in regulator-to-regulator session, pursuant to paragraph 3, specific companies, entities, or individuals, and paragraph 8, consideration of strategic planning issues relating to regulatory, of the NAIC Policy Statement on Open Meetings. During this call, the Working Group received a brief presentation from NAIC staff on the history of NAIC privacy models, a review of the Privacy Protections (H) Working Group's work over the past several years, and an update on the state privacy law landscape.

Kreiter made a motion, seconded by Smock, to adopt the Working Group's 2023 Fall National Meeting minutes (*refer to NAIC Proceedings – Fall 2023, Privacy Protections (H) Working Group*). The motion passed unanimously.

2. Heard a Presentation from Husch Blackwell on Federal and State Privacy Legislative Efforts

During the 2024 leadership transition, Beard said the Working Group paused its work on the *Insurance Consumer Privacy Protections Model Law* (#674), but the public continued to show strong interest in privacy-related discussions. Therefore, she said the Working Group would continue to hold open calls as necessary, as well as regulator-only sessions to determine the best privacy regime to move forward and draft a new model law or s revision that reflects it. Beard said the Working Group is beginning the meeting with a subject matter expert (SME) who will enhance issues the Working Group will discuss moving forward. She also said that after taking a moment to refresh and recharge earlier this year, the Working Group is pleased to kick off its work in 2024 with a presentation on federal and state privacy legislative activities by one of the premier privacy experts in America.

David Stauss (Husch Blackwell) discussed state privacy laws, focusing on consumer data privacy laws, biometric privacy laws, and children's privacy laws. He said California was the first state to pass a consumer data privacy law (California Consumer Privacy Act of 2018—CCPA). He said some states adopted their own state-specific laws shortly thereafter using the Washington Privacy Act model as a framework even though Washington has not yet adopted it. Stauss said there are variations in the types of consumer rights provided by different state laws and that states have added additional provisions to their existing general data privacy laws, such as biometric data collection regulations.

Stauss described the various state privacy bills and laws, including those related to children's privacy, consumer health data, data brokers, and algorithmic discrimination. He said different states have passed or are in the process of passing their own privacy laws, creating a complex landscape of state laws and regulations with various definitions and requirements. He said the foundational principles of these laws include privacy policies, consumer rights to access, delete, correct, and report their data, as well as opt-out rights for targeted advertising and profiling.

Stauss discussed the concept of universal opt-out mechanisms in privacy law, which allows individuals to easily opt out of targeted advertising cookies on websites. He said these laws mention the development of a protocol called the global privacy control signal test, which sends a signal to websites indicating that the user has opted out of targeted advertising cookies.

Stauss highlighted the emergence of employee data regulations in states such as California and Colorado, indicating that more states may follow suit in applying privacy rights to employee data. He discussed a draft bill that has not yet been introduced and said that it is uncertain whether this bill will be passed. He said there are other bills related to children's privacy and online safety that are also being considered.

3. Discussed Other Matters

Kristin Abbott (American Property Casualty Insurance Association—APCIA) said she would like to introduce a model approach to the Working Group that was drafted by a coalition of industry trade associations over the past two years using the Privacy of Consumer Financial and Health Information Regulation (#672) as a framework. The coalition believes the approach contains key concerns that the Working Group and other stakeholders have. Cate Paolino (National Association of Mutual Insurance Companies—NAMIC) said this draft focuses on key concepts, including data minimization, consumer access and deletion of data, and limited exemptions for companies with less than 35,000 customers.

Chris Petersen (Arbor Strategies) said the coalition of health carriers that he represents also participated in producing the industry model draft. He asked for it to include a safe harbor for the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and asked the Working Group to look at adverse consequences. He said every state has passed some type of privacy law, and Model #672 already had many core privacy principles in it, so they built upon that foundation.

Weyhenmeyer said that following this meeting, the industry draft would be distributed to Working Group members, interested regulators, and interested parties (including consumer representatives) and would be posted to the Working Group's public web page. She said a new core privacy issues quick look tool would also be posted for public review. Weyhenmeyer said a notice would be sent following the call announcing a two-week comment period that would end May 30. She asked that all comments be submitted in writing and that the comments only refer to the plan for moving forward.

Swanson said he welcomes the effort to create something more acceptable to most states.

Tolga Tezer (Canopy Connect) asked if he could submit comments on the last exposure draft of Model #674. Beard said the comment period on that model expired, and the Working Group was accepting comments on the plan to move forward now.

Beard reminded attendees about the upcoming regulator-only call on June 6 and the next open call in mid-June.

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

SharePoint/NAIC Support Staff Hub/Committees/H Committee/Working Groups/Privacy/2024/Summer/Minutes-PrivacyWG051524.docx