

B. Privacy Protections (H) Working Group

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

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

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

C. Cybersecurity (H) Working Group

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

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

3. Adopted its 2025 Proposed Charges

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

COmmissioner 5 1

s b m . 2 T F-0.6 (.6)-2.t5 (t)1e0 T8)-2. w
Amann made a motion, seconded by Commissioner Conway, to adopt the Committee's 2025 proposed charges (Attachment Four). The motion passed unanimously.

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

Kate Stillwell (FireBreak Risk) discussed the concept of ember cast, a phenomenon responsible for 90% of home loss, according to fire

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

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

Jennifer Crutchfield (Clearcover) said that Clearcover is a private passenger auto (PPA) capiTc 0.00(e)2.7 (r1.5 (e)2.8 (ar)1

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

Lemonade has a model governance process that consdaod[(c)1.2 ((o)-4.5n)-5.8 (o)-.9 (d)-0.6 /P <</MCID 2 >>(n)0.177b (n)-

Draft: 12/3/24

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

The Big Data and Artificial Intelligence (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Denver, CO, on Nov. 17, 2024. The following Working Group members participated: Michael Humphreys, Chair, and Shannen Logue (PA); Doug Ommen, Co-Vice Chair (IA); Kevin Gaffney, Co-Vice Chair, and Mary Block (VT); Sian Ng-Ashcraft and Molly Nollette (AK); Richard Fiore (AL); Tom Zuppan (AZ); Ken Allen (CA); Michael Conway and Jason Lapham (CO); Wanchin Chou (CT); Karima M. Woods and Dana Sheppard (DC); Richie Frederick (FL); Shannon Hohl (ID); Julie Rachford and Joanna Colli (IL); Holly W. Lambert and Victoria Hastings (IN); Shawn Boggs (KY); Tom Travis (LA); Caleb Huntington and Jackie Horigan (MA); Kory Boone (MD); Sandra Darby (ME); Jeff Hayden (MI); Phil Vigliaturo (MN); Chlora Lindley-Myers and Cynthia Amann (MO); Colton Schanz and John Arnold (ND); Connie Van Slyke (NE); Christian Citarella (NH); Seong Gom (NJ); Hermoliva Abejar (NV); Matt Walsh (OH); Teresa Green (OK); Raven Collins (OR); Karl Bitzky (SC); Travis Jordan (SD); Emily Marsh (TN); Jane Byckovski and Cassie Brown (TX); Michael Peterson (VA); Jay Brown (WA); Tim Cornelius (WI); Juanita Wimmer (WV); and Lela Ladd (WY). Also participating was Melissa Robertsrn Tc -0.011 Tw 1(J 0.0003 Tw 0.2011 0 Td ( )5Tj -0.

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

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

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

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

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

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

Draft: 11/19/24

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

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

1. Adopted its July 29 Meeting Minutes

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

2. Heard a Presentation on How AI Is Used ... Technology (NIST) framework for managing these AI risks and noted the alignment ... on the Use of Artificial Intelligence Systems by Insurers. However, he noted the importance ... a structured framework that, while useful and necessary, is not sufficient. Rather, a ca... taken to prioritize and take action in proportion to the level of risk.

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

Prince closed by briefly mentioning that the use of third

Commissioner Humphreys responded by stating that a couple of consumer representatives will give a presentation to the Big Data and Artificial Intelligence (H) Working Group at the upcoming Fall National Meeting, and the Working Group anticipates

Draft: 12/3/24

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

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Denver, CO, Nov. 17, 2024

Draft: 11/26/24

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

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Denver, CO, Nov. 18, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair, and Eric Lowe (VA); Sian Ng-Ashcraft (AK); Chris Erwin (AR); Bud Leiner and Alena Caravetta (AZ); Damon Diederich (CA); Wanchin Chou (CT); Li (DE); Elizabeth Nunes and Matt Kilgallen (GA);
(o)-9.6 (r)-2.8 (k)-5.5 (i)-362 (n)-0.8 (u)-0.7 g (r)8 (o)-9.6 (u)-0.7 (p)-0.7 (0 A1.04 72 4571]T578)Tj -0.004 Tc 0.0
ncerns of stakeholders were addressed. He said the NAIC has the
ortal.

y Insurance Association (APCIA) delivered public comments on behalf of
evelopment of this portal and offering the organization as a resource as

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

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

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

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

attack. He explained that compromised credentials are used in supply chain attacks, data

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

Draft: 11/16/24

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

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met Oct. 30, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Julia Jette (AK); Leo Liu (AR); Damon Diederich (CA); Wanchin Chou (CT); Li (DE); Matt Kilgallen (GA); Lance H1 Tc 1M0 TJ 0 Tc 0 Tw 3[illegible] Working Group [illegible]

The motion passed unanimously.

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

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

Henry then provided a list of the top three risks and threats, including a caveat to suggest the overview is not exhaustive and an hour-long presentation could not fit such a list. Henry introduced the term business email compromise (BEC) and explained that Coalition Incident Response (Coalition) emp(l)24.73e ( )Tf(i)7T6 9 (t)47.9.5 0 (TC)(-)2.9 8
em

and discussion of cyber hygiene and cyber event prevention. Amann said there is still a need for good cyber practices, oversight, and continued education and that buying coverage is just the first step. She suggested collecting and analyzing cyber data.

Draft: 10/28/24

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

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met Oct. 8, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Julia Jette (AK); Leo Liu (AR); Lei Leiner (AZ); Damon Diederich (CA); Wanchin Chou (CT); Li (DE); Matt Kilgallen (GA); ( )Tj -0.00 Tc -0.001 Tw -43.2 0 85 [(()-11.M (ilg)2I

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

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

- Internet Crime Complaint Center

TmTf 0.002 Tc 1.326 0 Td [(I)4 (n)5.3 (ter)3.2 (n)5.2 (et C)2.4 (r)3N00eenu

Draft: 9/11/24

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

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met September 4, 2024. The following Working Group members participated: Cynthia Amann, Chair (MO); Michael Peterson, Vice Chair (VA); Chris Erwin (AR); Bud Leiner (AZ); Damon Diederich (CA); Wanchin Chou (CT); Li (DE); Matt Kilgallen (GA); Lance Hirano (HI); Daniel Mathis (IA); J. Metcalf (IL); Shane Mead (KS); Mary Kwei (MD);

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

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

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

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2024_4Q/H_WG-Cybersecurity/2024 0904 Interim Meeting/Minutes-CyberWG090424.docx

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

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

Oppenheim said Congress is continuing the discussion of a federal bac

Draft: 7/10/24

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

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

1. Heard a Presentation

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

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

Seymour provided reflections for state insurance regulators; the research has provided data-driven epiphanies of

The mission of the Innovati
insurance(p)2.2( )]Tp.J-36u T
providing assistance to state insurance regulators as needed
E. Coordinate and facilitate collaboration with and among c
promote consistency and efficiency in the development
enforcement materials and tools related to innovation, cy
technologies, big data, and artificial intelligence (AI), includi
insurance. Evaluate and recommend certifications, continuin
staff related to technology, innovation, cybersecurity, and da
F. Follow the work of federal, state, and international govern
and practices.