INNOVATION, CYBERSECURITY, AND TECHNOLOGY (H) COMMITTEE

Innovation, Cybersecurity, and Technology (H) Committee March 25, 2026, Minutes
- Big Data and Artificial Intelligence (H) Working Group March 24, 2026, Minutes (Attachment One)
  - Big Data and Artificial Intelligence (H) Working Group Feb. 17, 2026, Minutes (Attachment One-A)
  - Big Data and Artificial Intelligence (H) Working Group Feb. 9, 2026, Minutes (Attachment One-B)
- Third-Party Data & Models (H) Working Group March 23, 2026, Minutes (Attachment Two)
  - Third-Party Data & Models (H) Working Group Feb. 26, 2026, Minutes (Attachment Two-A)
- Cybersecurity (H) Working Group March 24, 2026, Minutes (Attachment Three)
  - Cybersecurity (H) Working Group March 13, 2026, Minutes (Attachment Three-A)
    - Adopted Centralized Cybersecurity Event Notification Portal Project Document (Attachment Three-A1)

Draft Pending Adoption

Draft: 4/1/26

Innovation, Cybersecurity, and Technology (H) Committee
San Diego, California
March 25, 2026

The Innovation, Cybersecurity, and Technology (H) Committee met in San Diego, CA, March 25, 2026. The following Committee members participated: Michael Yaworsky, Chair (FL); Karima M. Woods, Vice-Chair represented by Dana Sheppard (DC); Heather Carpenter (AK); Mark Fowler (AL); Jimmy Harris (AR); Michael Conway represented by Jason Lapham (CO); Ommen (IA); Jon Godfread represented by Colton Schulz (ND); Eric Dunning (NE); Michael Humphreys (PA); Bill Huddelston (TN); and Kaj Samsom and Mary Block (VT). Also participating were: Lori Dreaver Munn (AZ); Josh Hershman, George Bradner, and Kristin Fabian (CT); Sandra Darby (ME); Christian Citarella (NH); Tom Botsko (OH); Elizabeth Kelleher Dwyer and Matthew Gendron (RI); Amanda Crawford (TX); Scott A. White and Michael Peterson (VA); and Nathan Houdek (WI).

1. Adopted its 2025 Fall National Meeting Minutes

Schulz made a motion, seconded by Fowler, to adopt the Committee's Dec. 11, 2025, minutes (*see NAIC Proceedings – Fall 2025, Innovation, Cybersecurity, and Technology (H) Committee*). The motion passed unanimously.

2. Adopted the Reports of its Working Groups and Subgroup

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

Commissioner Houdek said that during the Working Group's meeting on March 24, the Working Group adopted its Feb. 17 meeting minutes.

The Working Group next received an update on the artificial intelligence (AI) systems evaluation tool pilot, which officially started earlier in March. Commissioner Houdek said that pilot states are using the tool to support a mix of market conduct exams, financial exams, and financial analysis, and that it is part of a more general regulatory inquiry. Pilot state regulators are maintaining regular communication and coordinating with companies to include the pilot, and the Working Group will provide public updates throughout the process. The pilot summary document can be found on the Working Group's web page.

The Working Group then received a presentation on operationalizing the NAIC's *Model Bulletin on the Use of Artificial Intelligence Systems by Insurers*. The presentation explained possible approaches to implement the model bulletin through governance documentation and oversight practices.

Finally, the Working Group heard a panel discussion on AI governance trends from Scott Kosnoff of Faegre Drinker and Anthony Habayeb at Monitaur. The panel discussed emerging best practices for AI governance, highlighted the importance of cross-functional governance committees, emphasized the need for strong AI inventory management, especially for high-risk systems, and underscored the value of risk-based triage, focusing governance resources on materially risky or high-impact AI use cases. The panelists framed AI governance as an evolving risk management discipline that should be integrated into existing enterprise controls and decision-making structures.

B. Privacy Protections (H) Working Group

Director Dwyer said that the Privacy Protections Drafting Group met Nov. 7, 2025, and Dec. 3, 2025, in regulator to regulator session to consider revisions to Article 6 of the *Privacy of Consumer Financial and Health Information Regulation* (#672). Following those discussions, regulators published proposed changes as part of a longer-term effort to reassemble the model and re-expose it for public comment.

There are now three articles left to look at. Article 7 was exposed for a 30-day public comment period earlier in March. After reviewing the comments on Article 7, the work will then transition to Article 8 and Article 1, which contain the definitions that the regulators will later have to consider.

Director Dwyer further said that the Working Group did not meet at the Spring National Meeting but will continue to meet virtually. She said that later, the drafting group will submit the full revised draft of Model #672 to the Working Group, after which, the Working Group will be able to take up additional comments at the end of this year.

C. Third-Party Data and Models (H) Working Group

Lapham said the Third-Party Data and Models (H) Working Group met March 23. During this meeting, the Working Group adopted its minutes and discussed potential revisions to the third-party regulatory framework. The exposed draft framework focused on company operations with direct consumer impact, including pricing, underwriting, utilization reviews, claims, fraud, and marketing. He said that during the meeting, the Working Group reached consensus to narrow the focus to pricing and underwriting as a first step.

Lapham said this process would continue to be iterative and noted that the registration process is better described as a registry. He said that the Working Group had reached consensus on the third-party data and models registry, focusing on the governance review of the datasets and models. The registry will provide a market view of third-party activities and gather information from third parties about their data and model governance. The registry would contain information so that third parties could validate those third parties operating in the insurance space. The registry concept represents an initial step that enables regulators to verify consistent national governance standards across third parties, thereby strengthening consumer protection.

The Working Group also met March 19 and Feb. 5 in regulator-to-regulator session, pursuant to paragraph 3 (specific companies, entities, or individuals) of the NAIC Policy Statement on Open Meetings, to continue work on its goals.

D. SupTech/GovTech (H) Subgroup

Munn said that since the SupTech/GovTech (H) Subgroup focuses on regulatory tools and education, and receives feedback from companies on proprietary technology, the meetings are conducted in regulator-to-regulator session.

The Subgroup continues to use the results of the regulator survey conducted last year to identify topics that drive efficiency, reduce administrative burden, and strengthen regulatory effectiveness.

Munn said that since the 2025 Fall National Meeting, the Subgroup met March 3 to receive presentations from three insurance departments on their work to create and foster their data and analytics teams. Departments also shared their experiences interacting with insurance companies on their use of AI.

E. Data Call Study Group

Schulz said that the Study Group continues to modify its approach to meet evolving priorities in other committees. The Study Group began with a plan to develop a manual inventory of all NAIC data elements, including definitions, but quickly recognized this was a case of boiling the ocean. The Study Group's efforts are now focused on market regulation data elements, but it has an automated approach for creating the data inventory. The Study Group's work relies on metadata within the NAIC's enterprise data platform, which is an ongoing project for NAIC committee support to flesh out, including adding business descriptions for the database and column names. An initial inventory has now been generated and provisioned in NAIC's ThoughtSpot tool. It includes Market Conduct Annual Statement (MCAS) data, complaints data, and the homeowners data call. Schulz said he would be reviewing the draft inventory before providing it to regulators. He will then work with committee support to collect information about state ad-hoc data calls, including those using the NAIC's Regulatory Data Capture tool and those performed outside of the NAIC.

Schulz also said that later, committee support will incorporate financial statement data elements into the data inventory. All of this work will then be used to identify data gaps.

Commissioner Ommen made a motion, seconded by Director Carpenter, to adopt the reports of the: Big Data and Artificial Intelligence (H) Working Group (Attachment One), including its Feb. 17 and Feb. 9 minutes; Third-Party Data and Models (H) Working Group (Attachment Two), including its Feb. 26 minutes; SupTech/GovTech (H) Working Group; and Data Call Study Group. The motion passed unanimously.

3. Received an Update on the Cybersecurity Event Notification Portal and Adopted the Report of the Cybersecurity (H) Working Group

Commissioner Yaworsky discussed the ongoing work by the Cybersecurity (H) Working Group. He said that the Working Group has been leading discussions to develop a cybersecurity event notification portal. Departments of insurance (DOIs) currently receive cybersecurity event notices directly, and this application would allow the DOIs to receive such notices through the NAIC. Recognizing that some members of the Committee were relatively new to the discussion, Commissioner Yaworsky said he wanted to discuss this project to raise awareness of its components, anticipating a future Committee meeting to consider adoption.

Peterson also provided an update on the Working Group's activities. He said that the Working Group met at the 2025 Fall National Meeting to hear comments from members, interested state insurance regulators, and interested parties of the Working Group on the cybersecurity event notification portal project intake form and to hear a brief presentation on the NAIC's 2025 Cyber Insurance Market Report.

The Working Group then met Feb. 6 in regulator-to-regulator session, pursuant to paragraph 4 (internal or administrative matters of the NAIC) of the NAIC Policy Statement on Open Meetings, to discuss the revised version of the cybersecurity event notification portal project intake form and expose it for a public comment period.

The Working Group then met March 13. During this meeting, it reviewed and adopted revisions to the cybersecurity event notification portal project document following the most recent public exposure. He said that key updates include the addition of a draft standard reporting form, clarifications that licensees will not be charged to use the portal, and refinements to the Service Organization Control (SOC) 3 related language, which is a security report the NAIC will make available to stakeholders once the portal is operational. Industry stakeholders expressed general support for the project and appreciation for collaboration while identifying issues such as regulator access, data governance, concentration, risk, and confidentiality that will be addressed as technical details are developed. He said the Working Group unanimously adopted the revised project document as exposed.

Commissioner Yaworsky stated that the Committee plans to consider its own adoption of the project proposal at an April meeting to be announced and asked that Committee members reach out to speak to Peterson if they have questions about the project.

Schulz made a motion, seconded by Director Dunning, to adopt the report of the Cybersecurity (H) Working Group (Attachment Three), including its March 13 minutes.

4. Heard a Presentation from PwC on Insurance AI Trends, Including Agentic AI Applications

The Committee heard a presentation from PwC on insurance industry AI trends. Scott Froseth (PwC) described how many insurers remain in a transitional phase, constrained by legacy technology architectures and data readiness issues. As a result, most organizations are currently deploying AI through incremental, point-solution use cases rather than undertaking broader operating model transformation. He noted that while leading insurers are beginning to experiment with more sophisticated agent-based workflows, the majority of carriers remain focused on foundational capabilities such as data quality, operating model alignment, governance structures, and workforce readiness.

Froseth explained that agentic AI differs from traditional generative AI in that agents are designed not simply to generate content, but to execute tasks and orchestrate workflows by combining large language models (LLMs) with automation and process management tools. These systems can learn from repeated interactions and improve over time. He emphasized, however, that current implementations generally preserve human-in-the-loop controls for higher-risk decisions, particularly in underwriting and claims handling. Examples were shared demonstrating how agents can accelerate operational tasks while maintaining clear human accountability for final determinations.

Froseth and Ilana Golbin Blumenfeld (PwC) stated that change management is an important part of implementation because if employees do not understand the strategy of using AI, they may default to continuing to operate without using the newly available tools.

The presentation also addressed emerging AI operating models within insurance organizations. Froseth described a progression from centralized AI governance structures toward more hybrid approaches as adoption matures. He observed that fully federated models can lead to challenges such as tool proliferation, inconsistent governance, and fragmented risk oversight, while fully centralized models may struggle to scale or meet business demand. Many insurers are now experimenting with hybrid models that balance centralized standards and guardrails with increased flexibility for business units as AI tools become more accessible to non-technical users. Blumenfeld said that centralized operating models sometimes leave units competing for resources, making it challenging to implement projects when teams lack access to expertise. However, generative AI allows business units to do more initial work.

Froseth and Blumenfeld then discussed the evolving risk landscape of agentic AI systems, highlighting new governance challenges, including emergent behavior when multiple agents interact, the potential for cascading failures, automation bias, and increased complexity in managing data access across interconnected systems. She noted that traditional AI governance frameworks—largely developed for static or narrowly scoped models—are insufficient for autonomous or semi-autonomous agent systems.

As a result, insurers are increasingly investing in observability, monitoring, and lifecycle management capabilities to support accountability, resilience, and cost control. Blumenfeld noted that if an individual agent is not designed to access a certain data set, companies need to account for an agent's ability to interact with other agents to access that same data. Thinking about governance frameworks, Blumenfeld said that while the AI principles and

strategy a company operates under may not need to change, inventory practices, risk registers, and processes to test, monitor, and track risks may need to be redesigned in light of the advent of agentic AI.

Transitioning to a discussion, Schulz asked how data governance considerations for agentic AI differ from those applicable to more traditional AI systems, and what regulators should be attentive to in practice. Blumenfeld responded that while core data governance principles remain unchanged, agentic systems introduce additional complexity because agents access, combine, and pass information across multiple data sources. She emphasized the importance of clearly defining access permissions, validating data sources, and understanding how agent orchestration could inadvertently circumvent existing controls, requiring more granular oversight than prior AI implementations. Froseth provided an example of working with an AI agent that was given human resources-related tasks, and they worked to ensure access was tiered and granted as appropriate, but thinking about salary information, the agent would have access to.

Commissioner Yaworsky also asked about the importance of responsible AI governance in an environment where insurers face pressure to rapidly deploy AI technologies. Blumenfeld explained that effective governance enables faster, more confident adoption by clarifying expectations for risk tolerance, roles, decision authority, and controls throughout the AI lifecycle. She noted that without such structures, organizations may either move too cautiously or adopt technology without fully understanding risks, potentially leading to consumer harm or operational disruption.

Commissioner Yaworsky said he has heard legislative discussions that tend to center on outcomes, and while that is important, it does not capture the full universe of responsible AI governance, or at least the full scope of a governance framework. Blumenfeld agreed, saying that the insurance life cycle includes many components that are each important, but also cautioned against relying on humans in the loop because of the imperfections that people also have.

Commissioner Hershman raised questions about whether AI governance approaches should be principles-based or prescriptive, with specific deviation thresholds, particularly when performance deviations occur. Blumenfeld stated that rigid, uniform thresholds are difficult to apply across diverse AI use cases and may not adequately reflect contextual risks, compensating controls, or data limitations. She noted that while prescriptive requirements may be appropriate in highly regulated or high-impact contexts, most AI systems require use-case-specific evaluation informed by system design, governance maturity, and the broader control environment, rather than relying on a single quantitative benchmark.

Froseth added that the risk may also vary based on whether the software is third-party software or internally developed. Commissioner Hershman wondered if, at some point, a deviation standard would become necessary. Froseth discussed an example of an AI model's test in which the AI achieved 90% accuracy, but on investigation, the errors were found to be related to human labeling of the data.

Commissioner Samsom asked whether PwC had predictions of AI failures in insurance or more generally, and how governance would respond. Froseth discussed how inappropriate access to production data might pose a risk. Commissioner Samsom then asked whether that might be a relevant consideration in relation to Commissioner Hershman's comments on deviation standards—seeking production data access.

Blumenfeld said she tends to see things optimistically, but remarked that the AI Incident Database provides a public register of AI failures, which may be instructive. In some instances, agent-pushed code has led to system failures, but organizations are thinking critically as they implement AI. Froseth provided an example of Amazon ceasing the use of AI for coding due to system issues AI coding caused.

Commissioner Fowler asked whether the presenters had any recommendations for regulators to consider as they continued their regulatory discourse. Blumenfeld remarked that regulators have a difficult job, as they need to develop and update regulatory frameworks in a rapidly changing environment. Blumenfeld recommended continued engagement with the industry and flexibility, but noted that risks will continue to evolve and may require further adaptation. Froseth talked about the role AI may play in helping transition skills and empowering less experienced staff.

5. Other Matters

Director Dunning then reminded meeting attendees about InsurTech on the Silicon Prairie which will include several Commissioners and a speaker from Open AI in attendance.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2026_Spring/H-Minutes/Minutes-H-Cmte032526-Final.docx

Draft: 3/31/26

Big Data and Artificial Intelligence (H) Working Group
San Diego, CA
March 24, 2026

The Big Data and Artificial Intelligence (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in San Diego, CA, March 24, 2026. The following Working Group members participated: Nathan Houdek, Chair, Timothy Cornelius, and Coral Manning (WI); Doug Ommen, Co-Vice Chair (IA); Mary Block, Co-Vice Chair (VT); Richard Fiore and Mark Fowler (AL); Jimmy Harris (AR); Lori Munn (AZ); Ken Allen (CA); Michael Conway and Jason Lapham (CO); Wanchin Chou (CT); Karima M. Woods (DC); Nicole Crockett (FL); Matt Kilgallen (GA); Weston Trexler (ID); Jack Engle (IL); Meggan Brumbaugh (IN); Shaun Orme and Shawn Boggs (KY); Caleb Huntington and Jackie Horigan (MA); Sandra Darby (ME); Kate Stojsih and Joe Stoddard (MI); Phil Vigliaturo (MN); Jo LeDuc (MO); Jacqueline Obusek and Angela Hatchell (NC); Colton Schulz and Matt Fischer (ND); Connie Van Slyke (NE); Christian Citarella (NH); Vanessa DeJesus (NM); Gennady Stolyrov II (NV); Avani Shah (NY); Matt Walsh (OH); Nicole Nash and Brian Downs (OK); Michael Humphreys (PA); Matt Gendron (RI); Andreea Savu (SC); Travis Jordan (SD); Emily Marsh (TN); Nicole Elliott and Amanda Crawford (TX); Eric Lowe and Michael Peterson (VA); and Lela D. Ladd (WY). Also participating was: Tregenza Roach (VI).

1. Adopted its Feb. 17 Minutes

The Working Group met Feb. 17 and took the following action: 1) adopted its Feb. 9 minutes; and 2) continued to discuss edits to the artificial intelligence (AI) systems evaluation tool and heard feedback from interested parties.

Block made a motion, seconded by Commissioner Ommen, to adopt the Working Group's Feb. 17 minutes (Attachment One-A). The motion passed unanimously.

2. Received an Update on the AI Systems Evaluation Tool Pilot

Commissioner Houdek stated that the AI systems evaluation tool pilot process began earlier in March and that all participating states have sent, or are in the process of sending, inquiries to their respective insurance companies. The group of pilot state insurance regulators is meeting weekly to share insights on anticipated responses and to receive training on data science, compliance, and governance concepts reflected in the tool. The decision on which companies to include in the pilot is up to each pilot state's domestic regulator. Participating states are engaging with their domestic companies in advance of sending the pilot inquiry to answer questions and ensure that companies understand the goals of the pilot process. Where a company is part of a group, the pilot state regulators are coordinating efforts, including reaching out to non-pilot states to raise awareness that the company is included in the pilot. In general, there is a mix of companies across the main product lines, with more property/casualty (P/C) and life insurers than health insurers being selected. Most of the pilot states selected one to 10 insurers, with two states sending inquiries to more than 10 insurers.

Commissioner Houdek said the Working Group will first focus on Exhibit A to provide regulators with an overview of how companies use AI across their business operations. Then, states could use questions from Exhibits B-D to diver deeper into AI use. Pilot states are using the tool in support of a mix of regulatory processes (market conduct exams, financial exams, financial analyses, and as part of a more general regulatory inquiry). Pilot state regulators are collaborating on their insights to learn from each other. Throughout the pilot, the Working Group anticipates developing a coordinated mechanism to solicit feedback from participating companies on the tool. Recognizing

the broad interest in this initiative among regulators, industry, and interested parties, members of this Working Group and NAIC committee support have provided updates on the pilot at seven different meetings during the Spring National Meeting, including the three actuarial task force meetings, and the Market Regulation and Consumer Affairs (D) Committee, Financial Condition (E) Committee, and Innovation, Cybersecurity, and Technology (H) Committee. The Working Group will be providing public updates throughout the pilot process.

3. Received a Presentation on How to Operationalize the NAIC Model Bulletin on the Use of AI by Insurers

Dorothy Andrews (NAIC) presented possible approaches to move from adopting the *NAIC Model Bulletin on the Use of Artificial Intelligence Systems by Insurers* to actively implementing it through concrete governance, documentation, and oversight practices. She emphasized the importance of shared definitions for AI, machine learning, AI systems, consumer harm, and risk classes so that supervision is consistent and comparable across jurisdictions and companies. She stated that an AI risk taxonomy should serve as a guide to the appropriate level of governance, testing, and regulatory scrutiny for different AI uses. She outlined expectations for standardized AI governance that clearly describe executive accountability, board oversight, model inventories, data sources, and risk management frameworks. She highlighted the need for transparency around both internal and external data, including data purpose, demographics, bias and missing-data analysis, and third-party contractual and auditability and transparency considerations.

Andrews stated that AI model cards could be a practical tool to summarize what models do, how they should be used, how they perform, and their assigned risk level. She stressed the importance of ongoing monitoring to detect and respond to model drift rather than treating approval as a one-time event, and that attention should be given to protected class inference and bias testing, including the identification of proxy variables, statistical and sociotechnical analyses, and a clear discussion of model and data limitations. She noted that effective AI oversight requires sufficient human capital and expertise for both insurers and state regulators to review reports, follow up on risks, and enforce consequences where expectations are not met.

Commissioner Ommen, referring to the AI risk taxonomy of harm, commented that he has heard from interested parties that risk from the use of third-party data is mainly associated with pricing and underwriting, and asked Andrews to confirm. Andrews agreed, especially when it comes to third-party data that is aggregated but not sufficiently scrutinized by insurance companies, which could create harm consumers.

Eric Ellsworth (NAIC Consumer Representative) commented that two operational issues deserve attention. First is workflow integration, which refers to how an AI model is integrated into an insurance-related process. He stated that Andrews' presentation flags some impedance-mismatch issues with using a model outside its trained purpose, which are exacerbated when integrated into other processes. A component of that is the loss of knowledge by people who used to do the process manually. A strong governance structure raises awareness of knowledge loss and establishes a proactive stance to manage it. Second, there is a need for well-defined exception-handling processes when a model cannot do something well that it was not trained to do. Andrews replied that part of a good governance framework is ongoing training.

David Snyder (American Property Casualty Insurance Association—APCIA) reemphasized that one of the strengths of the NAIC AI model bulletin is that it is based on established regulatory standards and stated that it is important to constantly tether to those standards. He asked whether confidentiality will continue to be assured, given the assumption that the AI systems evaluation tool will be used in market conduct and financial examinations. Commissioner Humphreys responded that the Pennsylvania Insurance Department will administer the tool in a financial analysis context, thereby preserving confidentiality.

Commissioner Ommen echoed that the Iowa Insurance Division will be administering the tool through the financial examination process, where confidentiality would be preserved. In a market conduct review, Iowa would administer the tool under its market examination authority, and confidentiality would be maintained.

4. Heard a Panel Discussion on AI Governance Trends

Scott Kosnoff (Faegre Drinker) and Anthony Habayeb (Monitaur) discussed emerging best practices for AI governance, emphasizing that effective governance is primarily a business enabler rather than a narrow compliance exercise. The speakers highlighted the importance of cross-functional governance for aligning business, technology, risk, and compliance stakeholders and creating shared accountability. They stated the need for strong AI inventory management based on the principle that organizations cannot govern systems they cannot see. Success in many cases can be achieved by establishing awareness of the inventory of AI systems in place. The cross-functional dynamic is enforcing conversations and enabling proper governance and AI implementation success. They noted increasing pressure from insurance companies on vendors to demonstrate transparent, credible AI governance, especially for high-risk systems. The goal for insurers should be to have a clear story to tell regulators about their governance practices, demonstrating their appreciation for potential risks and their mitigation efforts. They described mature AI governance programs as those that institutionalize critical thinking about potential harms, impacts, and failure modes, rather than relying solely on formal processes.

Miguel Romero (NAIC) asked how to account for operational risk, financial risk, and the risk of adverse consumer outcomes, and whether companies are implementing a single risk criterion or a specific criterion for each type of risk. Habayeb responded that there is a learning curve, with many things that should be asked and managed upfront. Triage should be performed to determine the materiality of potential consequences that should be handled downstream. For example, if a system has been inherently evaluated as high risk, it should be assigned a control to address the risk of bias and its mitigation. Also consider robustness and system resiliency in performing risk assessment as a good fundamental risk management approach. Kosnoff stated that his firm has worked with clients to develop an AI use-case intake form to be submitted to the governance committee, which includes questions about the potential impact on policyholders, applicants, employees, other constituents, and the company itself in concern of a weakened financial condition. This intake form forces critical thinking about what the governance committee is asking to review, institutionalizing it and providing a starting point for the governance committee to conduct its review and determine where time and energy should be spent. Habayeb responded that the committee cannot reasonably review everything, so triage upfront is important for mitigation. Commissioner Houdek acknowledged that the tool's scope is intentionally broad at this point, but that it may be narrowed as a result of the pilot process.

Block asked the panel whether they are seeing any stratification by product line or company size in how well governance is progressing and maturing, and whether they are noticing any particular areas within companies that are driving the governance work. Kisnoff responded that he has not seen a stratification. Habayeb responded that large organizations tend to staff more full-time resources, but this may not be the case as much for regionals and smaller carriers, where the burden is larger. Kosnoff stated that it is hard to overemphasize the importance of education and training and stated that like the concern for model drift, there is a concern about human drift, when the people start to cut corners, get stressed, run short on time, get complacent, and become overly reliant on machines to make recommendations or determinations, which poses a compliance risk for all organizations.

Stolyrov II asked the panel for their insights on the extent to which a taxonomy of harm has become embedded in insurers' cultures, and whether to adopt a particular model. If an insurer could prioritize controls to prevent a

large amount of shock and outrage by consumers, prevent consumer complaints, regulatory actions, and litigation in the longer term, then that is a profitable series of moves, and ask whether they are seeing insurers think in these ways. Habayeb reinforced his earlier point that performing an intake assessment is an exercise in thinking about business impact.

5. Heard a Federal Update on AI

Shana Oppenheim (NAIC) said that on March 20, 2026, the White House released a National Policy Framework for Artificial Intelligence, outlining policy recommendations to guide Congress in developing a unified federal approach to AI legislation and regulation. The policy recommendations are consistent with what the Trump administration has been signaling about its views for some time: 1) the proliferation of state AI laws is creating barriers to innovation; 2) there needs to be some national standard governing AI; and 3) there are particular areas in which Congress should act in order to protect individuals from potential individual and economic harms that could be caused by the continued adoption of AI technologies.

Oppenheim added that last summer, the Trump administration urged Congress to adopt a temporary federal moratorium preempting certain state AI laws, but Congress ultimately declined to pursue that approach. Shortly thereafter, in December 2025, the administration issued Executive Order 14365, establishing a national policy framework for AI and seeking to curtail the impact and continued proliferation of state AI regulation. Among other elements, this Executive Order directed the Department of Justice to establish an AI litigation task force and instructed federal agencies to assess whether discretionary funding programs could be used to discourage certain types of state AI regulation. The Executive Order committed the administration to working with Congress to develop a federal legislative framework that would replace most state-level AI laws with a unified national standard. The framework released on March 20 follows up on that commitment by outlining the administration's preferred approach to federal AI legislation, providing guidance on the key areas that any federal legislation should address and the categories of state AI laws that should be preempted.

While the framework spans a wide range of policy areas organized around six key objectives, the following takeaways are important for companies that develop, augment, deploy, or test AI systems:

1) Child Safety and Privacy Regulation: A significant focus of the framework is protecting minors from AI harms and empowering parents to control their children's digital environments. The Framework encourages Congress to adopt age-assurance requirements for AI platforms likely to be accessed by minors, tools that can be used by parents and guardians to manage privacy and engagement settings, and limits on data collection and online behavioral advertising. The framework urges pursuing these goals while avoiding ambiguous content standards or open-ended liability regimes that could drive excessive litigation.
2) Copyright, Fair Use, and the Judiciary: The framework acknowledges the judiciary's authority to assess copyright and fair use questions related to AI training, while noting the administration's view that training AI models on copyrighted material does not violate copyright laws.
3) Antitrust Liability Exemption for Collective Licensing Negotiation: The framework encourages Congress to consider enabling licensing or collective-rights frameworks that would allow intellectual property rights holders to collectively negotiate compensation from AI model developers without incurring antitrust liability.
4) Free Speech Protection: The framework emphasizes limits on the federal government's authority to coerce AI providers to restrict or alter content for partisan or ideological reasons. It also directs Congress to provide avenues for redress where such coercion occurs.

5) No New Federal Rulemaking Body: The framework encourages relying on existing sector-specific regulators and industry-led standards rather than creating a new, centralized federal AI regulatory authority.
6) Federal Preemption of State AI Regulation: The framework supports broad federal preemption of state AI laws that impose undue burdens, while preserving states' traditional police powers to enforce laws of general applicability, especially to protect children, prevent fraud, and safeguard consumers. Additionally, the framework calls for precluding states from regulating AI model development or imposing liability on AI developers for unlawful conduct by third parties using their systems.

Oppenheim concluded that the framework is not a binding document and, by itself, does not impose new legal obligations or direct agencies to take specific regulatory actions. Instead, it outlines a series of recommended policy approaches for Congress to consider in drafting comprehensive federal AI legislation.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2026_Spring/WG-BDAI/Spring-Minutes/Minutes-BDAIWG-032426 - Final.docx

Draft: 2/24/26

Big Data and Artificial Intelligence (H) Working Group
Virtual Meeting
February 17, 2026

The Big Data and Artificial Intelligence (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met Feb. 17, 2026. The following Working Group members participated: Nathan Houdek, Chair, Lauren Van Buren, Coral Manning, and Timothy Cornelius (WI); Doug Ommen, Co-Vice Chair, Daniel Mathis, and Amanda Theisen (IA); Mary Block, Co-Vice Chair (VT); Molly Nollette and Alex Romero (AK); Tom Zuppan (AZ); Ken Allen (CA); Jamie Crise (CO) Wanchin Chou and George Bradner (CT); Karima M. Woods (DC); Stuart Jones (FL); Matt Kilgallen (GA); Weston Trexler (ID); Jack Engle (IL); Chris Cerniauskas (LA); Caleb Huntington and Jackie Horigan (MA); Mary Kwei (MD); Kate Stojsih (MI); Phil Vigliaturo (MN); Brad Gerling (MO); Jacqueline Obusek (NC); Colton Mork (ND); Connie Van Slyke (NE); Christian Citarella (NH); Vanessa DeJesus (NM); Nishtha Ram (NY); Matt Walsh (OH); Landon Hubbart (OK); Michael Humphreys (PA); Matthew Gendron (RI); Andreea Savu (SC); Travis Jordan (SD); Michael Schulz (TN); Eric Lowe (VA); and Lela D. Ladd (WY).

1. Adopted its Feb. 9 Minutes

The Working Group met Feb. 9 and took the following action: 1) adopted its Dec. 7, 2025, minutes; 2) discussed an update on the pilot process of the artificial intelligence (AI) systems evaluation tool; and 3) discussed edits to and heard feedback on the AI systems evaluation tool.

Commissioner Ommen made a motion, seconded by Lowe, to adopt the Working Group's Feb. 9 minutes (Attachment One-B). The motion passed unanimously.

2. Discussed Edits to the AI Systems Evaluation Tool and Heard Feedback from Interested Parties

Commissioner Houdek announced that Maryland and Louisiana have decided to participate in the pilot process, bringing the total to 11 states, and that the Working Group has heard requests from some trade groups and interested parties for more regular updates.

Karin Gyger (American Council of Life Insurers—ACLI) questioned the intent of the sentence in the third paragraph of Exhibit B ("The references to, and questions about, elements of an AI governance and risk assessment framework in this Exhibit B do not create a requirement that an AI governance and risk assessment framework is inadequate"). Commissioner Houdek responded that the Working Group will revise that sentence.

Gyger commented that the Working Group added a new sentence regarding AI models that augment or automate. ACLI members request that "augment" be deleted from Exhibit A and that the definition of augmentation be deleted, as it could broaden the scope to essentially anything that augments decision-making related to consumers, which the ACLI believes goes beyond direct consumer impact. Commissioner Houdek responded that the Working Group will keep the wording as is, with the intent to keep the language broad in order to collect information, but may narrow the scope based on feedback from the pilot experiences.

Commissioner Houdek stated that there will be an opportunity to provide additional comments before any vote is taken to finalize the tool. The intent of the pilot process is to keep the scope broad to collect as much information as possible, with the intent that the feedback from the pilot states will help refine and narrow the scope, and that there will be an opportunity for comments later this year before the tool is finalized.

Miguel Romero (NAIC) credited Manning, who suggested the proposed wording to the effect that elements of a company's AI systems governance risk assessments are not intended to create new requirements.

Dave Snyder (American Property Casualty Insurance Association—APCIA) noted his concern that companies may be subject to repetitive requests from different states. He stated that he looks forward to the most efficient and expeditious way to perform the pilot. He noted that several places in the tool mention "directly" or "indirectly," and that the mention of "indirect" concerns APCIA member companies. He also noted that the reference to ensuring the ethical use of AI Systems should be replaced with a tie back to state and federal laws and regulations. He was concerned that the definition of "externally-trained models" might be too broad to include general-purpose generative AI, and suggested that the definition exclude foundational generative AI. He noted a concern about tying complaints back to the AI system or model that was the subject of the complaint. Commissioner Houdek stated that most of those edits had already been made, but noted that his concerns will be taken into consideration.

Romero commented that the distinction between direct and indirect can be blurry and may warrant further conversation.

Ladd asked whether the questions in the Tool would create new regulations or requirements. Romero responded that it should be clarified that the Tool does not intend to create new regulations or requirements.

Miranda Motter (AHIP) expressed the desire that the pilot states coordinate the administration of the Tool consistently and be mindful of insurer holding company structures to avoid duplicative requests to the same legal entities. She asked for the incorporation of a formal, structured input intent in the background document, so that it can be reported out as part of the pilot to further strengthen the evaluation and ongoing improvement of the tool. She noted that it is important to consider annual statement filing obligations when timing the administration of the Tool. Commissioner Houdek responded that the goal is for the pilot states to coordinate as much as possible.

Randi Chapman (Blue Cross Blue Shield Association—BCBSA) reiterated the importance of cooperation among the pilot states to avoid duplicative and conflicting requests and the concern about conflicting with the annual statement filing season. Commissioner Houdek appreciated the busy time period currently and noted the pilot should start after March 1.

Lindsey Stephani (National Association of Mutual Insurance Companies—NAMIC) commented that it would be more appropriate to narrow the definition of predictive models to models that incorporate or use machine learning (ML). She said she will send written comments regarding the definition. She said it would be helpful to understand the reason the generalized linear model (GLM) definition was removed from a prior version. She noted the importance of regular public reporting of both feedback and experience with the pilot to interested parties. Commissioner Houdek noted that the Tool is still a draft, and the Working Group is still taking requested edits.

Commissioner Houdek concluded by stating that the Working Group anticipates finalizing the Tool shortly for pilot use and that the pilot states will coordinate as much as possible during the pilot process in order to learn about further refinements needed. The goal is to finalize the Tool for consideration for adoption at the Fall National Meeting.

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

Draft: 2/19/26

Big Data and Artificial Intelligence (H) Working Group
Virtual
February 9, 2026

The Big Data and Artificial Intelligence (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met Feb. 9, 2026. The following Working Group members participated: Nathan Houdek, Chair, Lauren Van Buren, Coral Manning, and Timothy Cornelius (WI); Doug Ommen, Co-Vice Chair, Daniel Mathis, and Amanda Theisen (IA); Mary Block, Co-Vice Chair (VT); Molly Nollette (AK); Richard Fiore (AL); Lori Dreaver Munn and Tom Zupan (AZ); Ken Allen (CA); Jason Lapham (CO); Wanchin Chou, Kurt Swan, and George Bradner (CT); Shannon Hohl (ID); Nicole Crockett (FL); Jack Engle (IL); Shaun Orme (KY); Nathan Strebeck (LA); Jackie Horigan and Caleb Huntington (MA); Raymond A. Guzman (MD); Sandra Darby (ME); Kate Stojsih (MI); T.J. Patton (MN); Julie Lederer (MO); Colton Schulz (ND); Connie Van Slyke (NE); Christian Citarella (NH); Randall Currier (NJ); Kevin Yan (NY); Michael Humphreys and Diana Sherman (PA); Matt Walsh (OH); Matthew Gendron (RI); Travis Jordan (SD); Michael Schulz (TN); Rachel Cloyd (TX); Eric Lowe (VA); Joylynn Fix (WV); and Lela D. Ladd (WY).

Opening Remarks

Before addressing the meeting's agenda, Commissioner Houdek acknowledged that Commissioner Humphreys has stepped back from serving as chair of the Working Group in 2026. He thanked Commissioner Humphreys for his leadership in 2025 and for advancing the work and progress on the artificial intelligence (AI) systems evaluation tool. He also expressed thanks that Commissioner Ommen and Block will remain as Co-Vice Chairs.

1. Adopted its Dec. 7, 2025, Minutes

The Working Group met Dec. 7, 2025, and took the following action: 1) adopted its Nov. 19, 2025, minutes; 2) discussed feedback, reactions, and revisions to the AI systems evaluation tool; and 3) discussed the pilot process of the AI systems evaluation tool.

Darby made a motion, seconded by Munn, to adopt the Working Group's Dec. 7 minutes (*see NAIC Proceedings – Fall 2025, Innovation, Cybersecurity, and Technology (H) Committee, Attachment Two*). The motion passed unanimously.

2. Discussed the AI Systems Evaluation Tool Pilot Process

Commissioner Houdek stated that the Working Group held a preliminary discussion on the AI systems evaluation tool pilot process at the 2025 Fall National Meeting and asked that Miguel Romero (NAIC) summarize the details. Romero stated that the participating states selected themselves and coordinated with the NAIC, with the goal that the pilot experience would help determine the tool's effectiveness and provide insight into how companies implement AI governance processes. He noted the timeline and how the tool will be used in the context of market conduct exams, reviews, financial analysis, and financial exams. Regulators have the freedom to tailor the tool, and based on company responses, the dialogue may shift. Regulators will focus on sending the tool to their domestic insurers, but each state will make its own decision. Regarding confidentiality, states will leverage their exam authority. As the pilot advances, the NAIC will provide updates to the Working Group, as well as other committees and stakeholders. The Working Group hopes to finish development of the tool for the pilot in February and publish it in March. Then, the Working Group will continue with training and share updates at the Spring National Meeting. The tool will be updated based on the pilot experience and potentially adopted at the Fall National Meeting. It is anticipated that there will be additional opportunities for public input.

Commissioner Houdek stated that this pilot process is an opportunity to learn what does and does not work, as well as what needs to be refined in order to finalize the tool and possibly adopt it later this year.

Karin Gyger (American Council of Life Insurers—ACLI) asked whether insurance company participation would be voluntary and whether the findings from the pilot would be subject to compliance penalties. Commissioner Houdek responded that the pilot states are discussing how the pilot will be structured and said he believed that participation will not be voluntary for selected companies. The pilot states will determine which companies to focus on and coordinate to ensure that companies do not receive multiple inquiries or correspondence from different states. Romero added that it will be a state-by-state decision that will be discussed with potential insurance companies, as governance is a currently developing implementation. Commissioner Houdek added that states will work with companies to gather information that will be beneficial in the long term.

Dave Snyder (American Property Casualty Insurance Association—APCIA) commented that it is unusual that participation would not be voluntary for the companies and regulators, and asked whether there is a way to collect member responses, questions, and concerns about the process. He also asked how to communicate with the pilot states and whether the Working Group intends to bring recommendations from the pilot to both the Financial Condition (E) Committee and Market Regulation and Consumer Affairs (D) Committee. Commissioner Houdek expressed that the Working Group appreciates feedback from industry on the experience, and if a company does not feel comfortable sharing directly, then it can share it through a trade organization. Regulators from the pilot states will meet regularly throughout the pilot process to share feedback. There will be an opportunity for more industry input on the tool once the pilot concludes.

Miranda Motter (AHIP) asked for clarity on the pilot process timeline and whether it will align with a financial exam schedule. Commissioner Houdek responded that the pilot states are coordinating among themselves on administering components of the tool and how it will be utilized through examination processes, but not every state may take that approach.

3. Discussed Edits to the AI Systems Evaluation Tool and Heard Feedback from Interested Parties

Commissioner Houdek stated that the Working Group held a half-day session at the 2025 Fall National Meeting, but was only able to discuss through Exhibit A. Since then, the drafting group has been working with NAIC staff to recommend edits to the remaining exhibits by incorporating the input and suggested edits from interested parties. He stated that the goal for the meetings today and next week is to continue discussing the remaining exhibits. Then, based on feedback from the pilot process, the Working Group will further refine the tool and provide an opportunity for additional input from interested parties, with the objective of finalizing and formally adopting it at the 2026 Fall National Meeting to then be utilized by states on a voluntary basis in 2027.

Romero highlighted some of the updated edits to the tool, including: 1) clarifying some of the language as suggested by the APCIA; 2) simplifying some of the governance framework questions; 3) focusing on material and direct impacts; 4) changing the word “ensure” to “evaluate” in several questions in Exhibit B (checklist); and 5) clarifying the reference to materiality, unfair discrimination, and how models were validated.

Block added that an insurance company should not be deterred from asking a regulator for clarification on the questions in the tool.

Romero stated that Exhibit D had fewer recommended edits, but some edits carried forward from other exhibits. The regulators are not ready to consider removing Exhibits C and D in response to some of the interested party feedback before those exhibits are tested. He stated that definitions were added for “augment,” “automate,” and “support,” and the definition for “neural network” was clarified.

Eric Ellsworth (NAIC Consumer Representative) noted that in practice, the distinction between "augment" and "automate" may be unclear. Commissioner Houdek requested that specific language changes be sent to Romero.

Wayne Turner (National Health Law Program—NHeLP) stated that he appreciated the added language on compliance that is not limited to the Unfair Trade Practices Act (#880), the addition of testing for compliance with unfair discrimination regulations, and the notion of accountability.

Lindsey Stephani (National Association of Mutual Insurance Companies—NAMIC) commented that the definition of "AI Systems" should exclude predictive models and generalized linear models (GLMs). Romero suggested the Working Group study and evaluate which models should be scoped in or out. Block suggested that the scope should still include GLMs, but that the pilot process would help determine whether it should be narrowed to exclude them, depending on the type of company and level of sophistication. Manning added that this should be considered on an individualized basis, depending on the company.

Ellsworth commented that "predictive" modeling is a use of a model, not a technique, and that many AI models are predictive. Stephani commented in support of Ellsworth but added that there is a distinction between true predictive models and AI. A predictive model could simply be rules-based or a simple algorithm and thus should not be in scope. Commissioner Houdek responded that the Working Group hesitates to scale back the scope, as it wants to keep it broad in the pilot phase and field testing to learn and refine the tool.

Huntington suggested that the term "predictive model" needs to be defined. Colton Schulz responded that this discussion may be getting lost in the details. He suggested that the inputs and outputs should be audited appropriately by the examiner, considering the context of the use of the model (i.e., predictive, AI, or otherwise).

Randi Chapman (Blue Cross Blue Shield Association—BCBSA) requested that the word "material" be added within Exhibit A, and "direct" be added within the question in Exhibit A regarding the number of AI System models with consumer impact. Commissioner Houdek responded that the Working Group does not want to narrow the scope but will discuss materiality further during the pilot process.

Snyder commented that the issue for companies is adding on to well-established regulatory standards and processes. He stated that he supports adding the concept of materiality and referring to consumer outcomes in a similar context to the model bulletin. He also pointed out that rating and underwriting factors are separately regulated. He added that the tool should focus on AI Systems that are new and different, not on back-office systems or models that have been long and effectively regulated by the states.

Motter asked whether the third-party data source and vendor name referenced in Exhibit C can be optional, given confidentiality agreements and disclosure obligations. Block responded that the issue will be discussed between the examination staff and the company.

Romero asked that additional edits from interested parties be sent in writing. Commissioner Houdek stated that additional edits can be discussed during the Working Group's Feb. 17 meeting. Based on that discussion, the Working Group will update the tool to ensure it is ready for the pilot process beginning in March.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2026_Spring/WG-BDAI/2026 0209Interim-Meeting/Minutes-BDAIWG-020926 - Final.docx

Draft: 4/1/26

Third-Party Data and Models (H) Working Group
San Diego, California
March 23, 2026

The Third-Party Data and Models (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in San Diego, CA, March 23, 2026. The following Working Group members participated: Jason Lapham, Chair (CO); Nicole Crockett, Vice Chair (FL); Molly Nollette (AK); Charles Hale and Richard Fiore (AL); Lori Dreaver Munn (AZ); Ken Allen and Chandara K. Phanachone (CA); George Bradner (CT); Grant Shintaku (HI); Doug Ommen and Jordan Esbrook (IA); Weston Trexler (ID); Julie Holmes (KS); Tom Travis (LA); Jackie Horigan (MA); Mary Kwei (MD); Sandra Darby (ME); Phil Vigliaturo (MN); Julie Lederer (MO); Colton Schulz (ND); Christian Citarella (NH); Gennady Stolyarov (NV); Kevin Yan (NY); Matt Walsh (OH); Ying Liu (OR); Michael McKenney (PA); Beth Vollucci and Matthew Gendron (RI); Andreea Savu (SC); Nicole Elliott (TX); Jessica Baggarley (VA); Mary Block (VT); and Timothy Cornelius (WI).

1. Adopted its Feb. 26 Minutes

Lapham stated that the Working Group met Feb. 26. During this meeting, the Working Group took the following action: 1) adopted its 2025 Fall National Meeting minutes; and 2) discussed the draft third-party regulatory framework and comments received.

The Working Group also met March 19 in regulator-to-regulator session, pursuant to paragraph 3 (specific companies, entities, or individuals) of the NAIC Policy Statement on Open Meetings, to discuss potential changes to the third-party framework.

Schulz made a motion, seconded by Vigliaturo, to adopt the Working Group's Feb. 26 minutes (Attachment Two-A). The motion passed unanimously.

2. Discussed Potential Revisions to the Third-Party Regulatory Framework

Lapham addressed what he described as a misunderstanding about the purpose of the third-party data and models registry. He said the original intent was to register the third-party vendors providing products and services to insurance carriers, not to require submission of models or datasets for review. The aim is to facilitate a direct connection between third parties and regulators. Crockett confirmed this, noting that registration was conceived as a lighter-touch alternative to licensure, avoiding compulsory examinations. Block added that the aim is not to create a comprehensive model review and data review framework that would result in everything getting approved and having to be filed by the third parties. Some noted that the existing draft framework language appears to be more heavy-handed. Lapham said the drafting group will make changes to better reflect the original intent. Commissioner Ommen highlighted the need for uniformity, where possible.

After discussion, the Working Group reached a broad consensus to narrow the initial scope of the framework to pricing and underwriting for the following reasons: 1) third-party vendor models are most prevalent and consequential in these areas; 2) states already have experience with vendor filings in this space; 3) the number and complexity of models per rate filing have grown significantly; and 4) underwriting should be discussed with rating because the distinction is mostly artificial, and quantitative models computing scores effectively perform rating functions regardless of label.

Working Group members noted that this prioritization should not foreclose future expansion to other functional areas (e.g., fraud detection, claims handling, marketing, etc.) and that the landscape will continue to evolve.

The Working Group agreed that governance should be the focus of registration. Key concerns raised include: 1) the adequacy of vendor governance programs; 2) the continuity of existence, including whether vendors will remain operational long enough to support the products carriers build around their models; and 3) longer-term solvency implications, particularly for life insurance products reliant on vendor-supplied models.

The Working Group discussed whether the registry should be voluntary or compulsory. This generated significant debate. Some members supported a voluntary process, as it would not require legislative changes and could start faster. States could still effectively compel participation by conditioning the use of vendor models on registration status. Members noted that the enforcement of registration requirements may not require legislation in many states, as regulators could simply decline to approve rate filings that rely on unregistered vendors. Several states indicated that they already apply this approach informally. Others supported compulsory registration because it better ensures comprehensive coverage. Several states noted that voluntary approaches have proven incomplete in past experiences. Questions arose about whether confidentiality protections that are often triggered by exam authority or compulsory submission would apply to voluntarily submitted information. Several members noted that without legislation, confidentiality protections for voluntarily submitted information may be insufficient to give vendors comfort in sharing sensitive data. No final decision was reached; the Working Group acknowledged that this is a key decision point requiring further analysis.

The Working Group discussed whether a registry could be created utilizing a centralized NAIC mechanism or whether it would need to be state-by-state. Stolyarov drew an analogy to the NAIC's *Quarterly Listing of Alien Insurers* under surplus lines, where states could refer to the NAIC voluntary registration framework when reviewing rate filings. Members noted that a nationwide registry could reduce duplicative burden on vendors filing across many states, create a shared information repository for regulators, and evolve over time without requiring immediate legislative changes. Questions were raised about who would review registrations for compliance, and whether a centralized mechanism would supplement or replace existing state registration requirements. No resolution was reached.

Lapham said a consensus was reached to: 1) utilize a governance approach with registration; and 2) narrow the framework's initial scope to pricing and underwriting. The drafting group will reconvene to map out key decision points (e.g., compulsory versus voluntary, model law versus guidance bulletin, centralized versus state-by-state, etc.), outline pros and cons, and bring a recommendation back to the full Working Group. The goal is to present a revised version of the framework for exposure by summer.

Having no further business, the Third-Party Data and Models (H) Working Group adjourned.

SharePoint/sites/NAICSupportStaffHub/MemberMeetings/HCMTE/2026_Spring/WG-Third-Party/Spring-Minutes/ 032326 Minutes TPDMWG SpNM.docx

Draft: 3/16/26

Third-Party Data and Models (H) Working Group
Virtual Meeting
February 26, 2026

The Third-Party Data and Models (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met Feb. 26, 2026. The following Working Group members participated: Jason Lapham, Chair (CO); Nicole Crockett, Vice Chair (FL); Alex Romero and Molly Nollette (AK); Lori Dreaver Munn (AZ); Ken Allen and Esteban Mendoza (CA); Wanchin Chou (CT); Doug Ommen, Julie Pearce, and Jordan Esbrook (IA); Weston Trexler (ID); Julie Holmes (KS); Caleb Malone (LA); Jackie Horrigan and Caleb Huntington (MA); Raymond A. Guzman (MD); Sandra Darby (ME); Phil Vigliaturo (MN); Brad Gerling (MO); John Arnold (ND); Christian Citarella (NH); Gennady Stolyarov and Brandon Rocchio (NV); Kevin Yan (NY); Matt Walsh (OH); Beth Vollucci and Matthew Gendron (RI); Andreea Savu (SC); Nicole Elliott (TX); Jessica Baggarley (VA); Mary Block (VT); and Timothy Cornelius (WI).

1. Adopted its 2025 Fall National Meeting Minutes

Crockett made a motion, seconded by Darby, to adopt the Working Group's Dec. 9, 2025, minutes (*see NAIC Proceedings – Fall 2025, Innovation, Cybersecurity, and Technology (H) Committee, Attachment Four*). The motion passed unanimously.

2. Discussed the Third-Party Regulatory Framework and Comments Submitted

Lapham stated that following the Working Group's Oct. 29, 2025, meeting, a small drafting subgroup consisting of regulators from Colorado, Florida, Iowa, Pennsylvania, and Vermont produced the first draft of the regulatory framework, which was shared during the 2025 Fall National Meeting. The framework applies across all lines of business (i.e., property/casualty [P/C] and life and health) and requires third parties to register with state departments of insurance (DOIs) if they meet the definition of a third-party data and model vendor and their data and/or models are to be used in an insurer's operations, which for now include pricing, underwriting, claims, utilization reviews, marketing, and fraud detection that have a direct consumer impact. To receive registered status, the third party would provide information about their governance program and agree to provide regulators with access to their data and models. Third parties would be afforded state confidentiality or trade secret status in the same way states apply their laws to insurers. In addition to registration, states may utilize a discretionary filing process if they wish to receive filings of data and models.

Lapham restated that the goals of the framework are to ensure regulators have timely access to information about third-party data and models used by an insurance company, and to confirm that third parties maintain strong governance practices to protect insurers and consumers. The framework was built in accordance with the concept of proportionality. Instead of a full licensure process, the drafting group proposed a registration process, which would give regulators the information they need without requiring a third party to become a licensed entity in each state.

The registration process consists of vendors registering, sharing details about their governance programs, and agreeing to provide regulators with access to relevant data and models. Once governance is approved, the vendor will then be officially registered by the state. From that point, insurers can use those models and data in the specific insurance company functions, unless a model or dataset is disapproved. In addition to registration, states may utilize a discretionary filing process if they wish to receive filings of data and models without reviewing every

dataset or model. For operations without direct consumer impact, existing insurer requirements apply as usual, and this framework would not apply.

Governance standards are outlined in the framework and would be developed over time. For third-party models, documentation includes the purpose, assumptions, inputs, limitations, performance metrics, and validation processes. For third-party data, documentation includes accuracy, completeness, timeliness, representativeness, auditable lineage, and quality controls. Third parties will be provided state confidentiality or trade secret status in the same way states apply their laws to insurers. Insurers will remain fully responsible for compliance. Registration of third parties would not relieve insurers of obligations. Insurers must validate model suitability, secure contractual access to necessary information, and meet all rating, underwriting, and other requirements—even when using third-party tools.

Lapham stated that the Working Group received comment letters from 23 interested parties during the exposure period. Overall, commenters generally supported responsible artificial intelligence (AI) oversight and consumer protection, but they believed the draft framework has flaws and requires revisions.

Lapham provided a summary of the comments received from interested parties of the framework as follows: 1) there was general support for consumer protection, but preference was for a risk-based, regulation; 2) oversight should focus on outcomes rather than processes; 3) many commenters had broad opposition to mandatory vendor registration requirements, citing concerns that it would reduce innovation, reduce competition, increase costs, and create operational and compliance burdens; 4) there was preference for voluntary vendor registration instead of mandatory requirements to encourage participation, improve transparency, and avoid regulatory burden; 5) there were concerns about legal authority and enforceability; 6) clarification should be made on the legal basis, enforcement mechanisms, and liability allocation; 7) concerns included confidentiality/trade secret protection, which could discourage participation; 8) concerns over the lack of clarity and overly broad scope, in particular that some terms are undefined, too broad, and/or ambiguous (e.g., “data,” "model,” “third-party vendor,” “direct consumer impact”); 9) concerns that the framework might cover basic software tools, public data sources, routine operational tools; 10) concerns about multistate regulatory differences; 11) existing oversight is currently sufficient, as insurers must currently conduct vendor due diligence, maintain governance frameworks, comply with the bulletin on the use of AI by insurers, and periodically undergo regulatory examinations; and 12) interested parties suggested an alternative approach of focusing on regulating insurers’ use of vendors.

Crockett commented that in light of the concerns raised, the Working Group does not intend to disturb the marketplace and will take the comments into consideration.

Chou commented that a senior manager or chief executive officer (CEO) may not have sufficient credentials to sign off on an attestation, but that a chief actuary or a chief data scientist would have the proper credentials.

Stolyarov commented that government data “pass-throughs” should be included because it is possible that insurance companies use the data outside of its original intent. He cited an example where a vendor provided auto violation information for insureds from the Nevada Department of Motor Vehicles (DMV) and other state DMVs to the Nevada DOI, but other states have different laws for commercial violations for other vehicles, which resulted in insurers using this data without understanding what would be chargeable under Nevada law. Thus, merely being a government “pass-through” of data should not absolve a vendor from scope.

Darby commented that: 1) the Maine Bureau of Insurance has concerns that the draft framework does not make it clear that the states will continue to require third-party models to be filed and approved prior to use; 2) the

section about third-party data should include how consumers can correct data errors; and 3) discussion needs to be held on where catastrophe (CAT) models fit into the framework.

Huntington commented that this discussion seems to focus more on P/C insurance than on health insurance, especially regarding utilization review. Lapham responded that these areas have been where the Working Group has seen the greatest use of third-party models and automation.

J.P. Wieske (American InsurTech Council—AITC) commented that, considering the large number of vendors that work with insurers, the AITC is concerned about the cost of compliance across all 50 states. Wieske stated that a consistent approach across states makes more sense, especially for smaller insurance companies, such as the Interstate Insurance Product Regulation Commission's (Compact) or the National Insurance Producer Registry's (NIPR's) licensing and registration processes, rather than 50 individual state vendors. Commissioner Ommen responded that the insurance industry is starting to see the promise of external third-party models. He said he hopes that small companies can rely on third-party models and technologies and that they are available across the market by making this registration process available to all companies.

Scott Harrison (AITC) commented that the most efficient way for small to mid-size companies to have access to technology and innovation is for insurance companies to conduct their own due diligence on third-party systems. Insurance companies should have good and robust governance policies. Harrison said the AITC believes the scope should be limited to P/C rating and underwriting, and the other use cases should be put off for another day. He urged states to learn from those already doing this.

Peter R. Kochenburger (Individual Consumer Advocate) questioned how the framework would stifle innovation. He stated that it is the insurance company's responsibility to ensure beneficial innovation, which does not mean sweeping away consumer protections but rather adapting them to future situations. The concern should be ensuring that regulators are able to perform their same oversight protection functions, not to reduce them.

Kristin Abbott (American Property Casualty Insurance Association—APCIA) commented that the proposed framework is unworkable, overly broad, and will likely produce outcomes that are counter to its objectives by limiting access to important tools, slowing innovation, and harming consumers. She commented that it will restrict access to third-party technologies and said she was concerned that vendors not exclusively focused on U.S. insurers would be unwilling or unable to comply, resulting in fewer technologies, slower innovation, and increased costs. Abbott further commented that: 1) the scope and definitions are too broad and risks sweeping in too many technologies and publicly available information; 2) the APCIA is concerned about state authority to regulate vendors; 3) the vendor regulation is not feasible for many vendors and could cut insurers off from their capabilities; and 4) confidentiality protections could fragment the national market. She urged the Working Group to address the foundational risks that are not currently addressed by the existing regulatory framework and refine the scope accordingly.

LaCosta Wix (AHIP) questioned state authority over third-party vendors and said she was concerned about the protection of confidential information and the effect of third-party registration on existing contractual relationships. Wix stressed the importance of consistency and application across states.

Lindsey Stephani (National Association of Mutual Insurance Companies—NAMIC) commented that: 1) the scope should be matched to the identified issue, which is specific to pricing and underwriting model vendors (not data); and 2) rather than a new framework, there might be some existing regulatory frameworks the Working Group could draw from. She mentioned that some jurisdictions allow non-licensed entities to file their models in the System for Electronic Rates & Forms Filing (SERFF), and she encouraged more discussion on this topic. She

suggested that the Working Group focus on facilitating access to information rather than registration, and she urged the Working Group to preserve confidentiality provisions.

Karin Gyger (American Council of Life Insurers—ACLI) commented that compulsory third-party registration is not necessary and recommended narrowing the scope to model vendors focused on providing models used for pricing, underwriting, and claims functions, but excluding data vendors in order to reduce complexity and improve consistency. She encouraged a voluntary, optional, registration-based framework where a vendor may elect to seek registration, because the ACLI is concerned that mandatory registration can stifle innovation, reduce participation, and create operational challenges.

Laura Panesso (Insurance Services Office [ISO]/Verisk) commented that limiting the scope to underwriting and rating will provide both benefits and efficiencies, and the framework should focus on activities with the greatest direct consumer impact. She added that although underwriting and rating are similar in nature, claims, marketing, and fraud detection come with additional and unique considerations, such as protection of fraud investigation activity, the wide range of claim types across life, health, and P/C, and even the diversity of marketing methods that could take considerable resources to address. Narrowing the scope to underwriting and rating also aligns with the current regulatory framework for product filings and can potentially leverage efficiencies within the current system. There are likely hundreds, potentially thousands, of third-party data and model vendors, and focusing on underwriting and rating will potentially limit the number of vendors required to register and potentially file, ultimately reducing the burden on regulators. Panesso reinforced the importance of confidentiality and stated that developing a model can take months or even years, and third-party model vendors invest considerable resources in developing their products. Protection of intellectual property supports innovation while providing transparency to regulators. The models, if made public through the filing process, could prove detrimental to the third-party vendors' businesses and potentially stifle innovation. Not all jurisdictions provide for confidentiality within the product filing framework, and ISO/Verisk encourages all jurisdictions to consider confidentiality protections beyond those that govern the traditional product filings.

Huntington commented that it seems like the discussion is focused more on P/C than on health, especially with regard to utilization review. Lapham agreed and added that utilization review on the health side is an area where the Working Group has seen the use of third-party models and automation of certain claims practices, and regulators have heightened concerns regarding the use of those tools in that space as well.

Lapham reiterated that the framework is explicitly designed not to require the submission of every model and every data set, and that it is up to each state's discretion. The amount of information requested for review is at the discretion of each jurisdiction.

Eric Ellsworth (Consumers' Checkbook/Center for the Study of Services) commented that it would be a mistake to create too many constraints on the scope of this framework too early in the process. Limitations on pricing and underwriting are more specific to P/C insurance than to health insurance. There are many use cases where risks can emerge that are not obvious up front. If a company contracts with a vendor providing poor-quality data, for example, from a large online data vendor for marketing or other uses, then large problems can occur without anyone understanding them. It would be unwise to limit the scope without considering those use cases and the serious risks. Additionally, a compulsory, lightweight registration process is not particularly burdensome, as it mimics client onboarding processes of filling out a registration form. Lastly, ultimately, there needs to be good governance on both sides, and diligence needs to be performed on governance by both the insurer and the regulator. In a startup environment, it is not always easy to know the risks. Part of the role of regulation is to move forward in this area, which ultimately accelerates product development, as seen in many other regulated industries. He said that good and early regulatory oversight directed toward the improvement of mitigating risks

that might not otherwise have been considered enables innovation. It would be unwise at this moment to limit the framework to specific insurer activities without thinking more broadly.

Erica Everson (Automotive Education & Policy Institute—AEPI) stated that registering third-party vendors is absolutely necessary. Regulators need the right to review and access third-party vendor software and modeling architecture. That is imperative because if issues are brought to regulators by consumers, the response from the regulatory authority is that they do not have the legislative mandate to be able to investigate how insurers made claims payment actions. She also urged the Working Group not to limit regulatory requirements to underwriting and rating. There is already a lack of transparency regarding insurer P/C mechanisms for determining claims valuations. As far back as 2003, when certain third-party vendors in the auto casualty and claims marketplace wanted to merge, the Federal Trade Commission (FTC) investigated one of the companies that stated that insurers have so much economic power over them that there is no possible way that they could engage in any antitrust activity, and that insurers require them to develop specialty software just for them and for the vendors as well, providing financing of $500,000–$600,000 to develop software for the insurers. The relationships between insurers and third-party model and data vendors are not necessarily independent.

Having no further business, the Third-Party Data and Models (H) Working Group adjourned.

SharePoint/NAICSupportStaffHub/Member Meetings/H CMTE/2026_Spring/WG-Third-Party/Minutes 022626 TPDMWG.docx

Draft: 4/2/26

Cybersecurity (H) Working Group
San Diego, California
March 24, 2026

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in San Diego, CA, March 24, 2026. The following Working Group members participated: Michael Peterson, Chair (VA); Colton Schulz, Vice Chair (ND); Alex Romero and Molly Nollette (AK); Mark Fowler and Richard Fiore (AL); Mel Anderson (AR); Lori Dreaver Munn (AZ); Damon Diederich (CA); Wanchin Chou (CT); Tim Li (DE); Matt Kilgallen (GA); Daniel Mathis (IA); C.J. Metcalf (IL); Shane Mead (KS); Nina Hunter (LA); Mary Kewi (MD); Danielle Torres (MI); T.J. Patton and Gregory Maus (MN); Kim Dobbs (MO); Troy Smith (MT); Jacqueline Obusek (NC); Martin Swanson (NE); Christian Citarella (NH); Vanessa DeJesus (NM); Peggy Willard-Ross (NV); Gille Ann Rabbin (NY); Matt Walsh (OH); David Buono (PA); Curt Kwak (WA); Jamie Adams (WI); and Lela D. Ladd (WY). Also participating was: Matthew Gendron (RI).

1. Adopted its March 13, 2026, and 2025 Fall National Meeting Minutes

The Working Group met March 13 and took the following action: 1) discussed proposed revisions to the portal project intake form and, subsequently, adopted the revised centralized cybersecurity event notification portal project document as exposed.

Mead made a motion, seconded by Chou, to adopt the Working Group's March 13, 2026 (Attachment Three-A) and Dec. 10, 2025, minutes (*see NAIC Proceedings – Fall 2025, Innovation, Cybersecurity, and Technology (H) Committee, Attachment Three*). The motion passed unanimously.

2. Heard a Presentation from CyberCube on Cyber Threats and Trends

Peterson noted that the Working Group successfully drafted and advanced the centralized cybersecurity event notification portal project document through the leadership of the Innovation, Cybersecurity, and Technology (H) Committee. Given this progress, Peterson indicated it was an appropriate time for the Working Group to receive presentations on current cyber threats and trends.

William Altman (CyberCube) described CyberCube's role in serving the global broker, underwriting, and reinsurance communities with data and analysis focused specifically on cyber risk from an insurance, reinsurance, and catastrophe modeling perspective. He noted that his team does not provide network defense services but instead focuses on understanding how cyber risk is evolving in ways that directly affect the insurance market. Altman also shared that his professional background is in cybersecurity threat intelligence, including work with government and Fortune 500 organizations, and that he has spent six years at CyberCube working closely with insurers.

Altman explained that the insights shared during the presentation were largely informed by CyberCube's concierge threat intelligence service, which is designed specifically to serve the insurance industry. He highlighted that this service includes annual threat briefings, as well as a CyberCube incident response capability that helps financial organizations understand large-scale cyber events in real time. Examples cited included major incidents such as the SolarWinds compromise and the Change Healthcare cyberattack. The presentation focused primarily on criminal cyber threats, particularly ransomware, as these threats are broadly applicable across organizations

of varying sizes. Altman noted that while nation-state threats are significant, criminal cyber activity remains the most pervasive risk for many enterprises. He indicated that he could address state-sponsored activity, including recent developments involving Iran, if there was interest.

Altman provided an overview of ransomware trends, explaining that ransomware includes both system encryption attacks and data theft combined with extortion. He emphasized that ransomware activity disproportionately targets the U.S., followed by the United Kingdom (UK), Canada, and France. He noted that this assessment draws on data from Recorded Future ransomware indicators of compromise combined with CyberCube's global enterprise intelligence data. The presentation highlighted that ransomware affects organizations across all industries, including manufacturing, health care, energy, and the public sector, and that any organization with digital connectivity faces exposure to this risk.

Altman further discussed emerging growth trends in ransomware outside traditional hotspots. When the U.S. and other highly digitized economies are excluded from analysis, the highest growth rates in ransomware activity are observed in emerging and fast-growing economies, including parts of Latin America and Africa. He attributed this trend in part to increased digitization and the use of generative artificial intelligence (AI) and large language models (LLMs), which allow threat actors to localize and scale attacks more easily. Using combined data sources, Altman explained that ransomware growth in certain regions correlates with factors such as corruption, weakened rule of law, limited criminal justice enforcement, and financial system opacity, all of which facilitate money laundering and reduce the likelihood of prosecution. These conditions create safe havens where criminal activity, including ransomware, can expand.

Altman also noted that ransomware activity has been observed to increase in and around conflict zones. Periods of heightened fear, uncertainty, and instability create conditions in which users are more likely to engage with malicious content. He cited examples, including countries affected by the Russia-Ukraine conflict, where ransomware has reportedly been used as a tool for economic destabilization, as well as regions in Africa and parts of Asia experiencing geopolitical tension. Altman observed emerging trends in ransomware activity in countries that have embraced digital currencies at the national level, noting that broader acceptance of cryptocurrency can affect how ransomware actors operate and transact.

Altman continued by noting that ransomware activity is elevated in countries where digital currencies are widely adopted at a national level. He explained that when organizations already hold bitcoin or have established mechanisms to transact in digital currency, the barrier for threat actors to collect ransom payments is reduced. As a result, countries with government-sanctioned or widely accepted cryptocurrency usage, including those with national bitcoin reserves or significant mining activity, have experienced heightened ransomware activity.

Altman emphasized that ransomware has increasingly become professionalized and militarized, particularly in and around conflict zones. He contrasted earlier ransomware activity, which tended to be opportunistic and unsophisticated, with today's more mature threat ecosystem. Beginning around 2020, threat actors shifted toward targeted attacks and, since that time, have developed vertically integrated criminal operations. These operations often involve distinct roles for initial access, lateral movement, data exfiltration or encryption, and ransom negotiation, forming a coordinated and specialized criminal ecosystem rather than isolated attacks. As these threat actors have become more capable, Altman explained that they are increasingly able and willing to target critical infrastructure. He cited examples across energy, utilities, transportation, logistics, and manufacturing sectors, including attacks that have disrupted ports, airports, gas facilities, and large manufacturing operations. He noted that cyberattacks are now producing real-world physical and economic impacts, extending beyond purely digital consequences.

Altman highlighted a recent attack he described as illustrative of these trends, particularly the blurring of criminal and state-sponsored activity. He explained that Iranian state interests often operate through or alongside criminal or so-called "hacktivist" groups, allowing them to damage adversaries economically while maintaining plausible deniability. As an example, he discussed an attack conducted by a group known as "Handala" against a Michigan-based health care company involving medical devices. He explained that the attack began with the compromise of user credentials due to inadequate credential hygiene, which allowed the attackers to gain privileged access. Once inside the network, the attackers abused a legitimate Microsoft Intune function to remotely wipe devices across the enterprise. Altman emphasized that this attack did not rely on zero-day exploits or highly advanced techniques, but instead it leveraged basic control failures and legitimate administrative tools. Despite this, it resulted in significant disruption to the health care system and illustrated how lapses in basic cyber hygiene can have severe societal consequences.

Altman then shifted focus to the growing impact of cyber threats on small businesses. He noted that criminal activity has been increasingly democratized through the use of AI tools, enabling attackers with lower skill levels to conduct damaging attacks at scale. Small and mid-sized businesses, particularly those with revenues in the approximate range of $10 million to $250 million, are increasingly targeted. He emphasized that these organizations often form the backbone of local and national economies and represent both a growing area of risk and a key opportunity for insurers and risk modelers. Altman indicated that this trend warrants close attention in 2026.

Altman briefly discussed CyberCube's ability to assess inherent cyber risk and security posture across companies and industries. He noted that some sectors, particularly health care and education in the small business context, exhibit higher inherent cyber risk than sectors such as financial services. He emphasized that organizations of similar size and geography can still present materially different cyber risk profiles, underscoring the importance of nuanced risk assessment.

Transitioning to emerging risks, Altman addressed the use of AI in cyber threats. He identified two major trends: 1) the increasing volume of machine-generated code relative to human-written code; and 2) the speed at which both vulnerabilities and attacks can now occur. He cited findings indicating that while generative AI can produce code rapidly, a significant portion of that code includes known security vulnerabilities, including those identified in the Open Worldwide Application Security Project (OWASP) Top 10. This creates the potential for vulnerabilities to be introduced at machine speed. At the same time, Altman explained that threat actors are dramatically reducing the time between initial network compromise and operational impact, such as data theft or system disruption. These trends are converging, resulting in an environment where both vulnerabilities and exploitation occur more quickly. As a result, he emphasized that organizations must shift focus toward visibility of internet-facing vulnerabilities and prioritize resilience and recovery. He stated that recovery speed is becoming more critical to limiting business interruption than purely detection or containment.

Altman encouraged organizations to prepare for worst-case scenarios through regular tabletop exercises and post-exercise evaluations, emphasizing resilience rather than resignation. He clarified that this approach is not an acceptance of inevitable failure, but rather an acknowledgment of the current threat environment.

Altman described the current phase of cyber threats as a "self-driving" era, in which human attackers retain strategic control while AI tools automate portions of the attack process. He explained that AI is being used to accelerate workflows and coordination rather than to fully automate attacks. While the concept of fully autonomous, or "agentic," AI-driven attacks remains speculative, he noted early indicators pointing toward a future in which automated attacker systems may increasingly contend with automated defensive systems.

Altman highlighted two recent incidents as key case studies for understanding how AI is shaping cyber threats: 1) activity observed by Anthropic involving a threat actor referred to as GTG-2002; and 2)AI-enabled mass exploitation of unpatched FortiGate devices observed in early 2026. He stated that these incidents demonstrate faster targeting, improved coordination, and increased automation, even without the use of novel exploits. Drawing lessons from these incidents, Altman emphasized the importance of identity security, including proper configuration of multifactor authentication (MFA), privileged access controls, and network segmentation. He also stressed the critical importance of timely patching, noting that traditional "patch when feasible" approaches are no longer sufficient for internet-facing systems, as threat actors are now able to identify and exploit vulnerabilities rapidly and at scale.

Altman reiterated that traditional approaches to vulnerability management, such as deferring patching with the expectation that threat actors may not discover a vulnerability, are no longer viable. He stressed that threat actors will identify and exploit vulnerabilities rapidly, particularly those that are internet-facing, and emphasized the importance of having a disciplined approach to patching early and often.

Turning to forward-looking considerations, Altman stated that organizations are already experiencing the impacts of AI in cyberspace and that these dynamics are accelerating, not slowing. He noted that cyber risk has often been treated as a force multiplier for existing loss patterns, but he suggested that AI-enabled threats may challenge those assumptions. He outlined several indicators that could help risk managers and underwriters assess whether cyber risk dynamics are fundamentally shifting. Altman identified the emergence of AI "agents" as a key trend to watch. He explained that organizations are beginning to deploy autonomous or semi-autonomous agents within enterprise networks to perform tasks on their behalf. He noted that this represents a significant evolution from prior technology deployments and is expected to scale substantially over the next several years. From a risk perspective, he emphasized that these agents may introduce privileged execution pathways within critical systems, creating new risks related to data theft or operational disruption. He stressed the importance of tracking whether AI systems are securely deployed and appropriately governed.

Altman also discussed the increasing enterprise adoption of advanced, or "frontier," AI models and the potential consequences of disruptions to those systems. He cited a lengthy outage of a major AI service in mid-2025 as an example, noting that impacts were limited at the time because AI tools are still largely used as assistants rather than as core decision-makers or controllers of operational infrastructure. He observed that as AI use cases increasingly integrate into critical operations and control environments, outages or failures are likely to carry more significant operational and economic consequences. He emphasized the importance of monitoring concentration risk and understanding dependencies on particular AI models or providers.

Altman summarized key issues for organizations to monitor as they look to 2026 and beyond, including the continued compression of attack timelines enabled by AI, the expansion of agentic AI within enterprise environments and the permissions and controls associated with those deployments, and aggregation risks within the AI supply chain stemming from concentration across a limited number of providers or platforms. He noted that CyberCube anticipates continued research and analysis in this area and expressed appreciation for the opportunity to present to the Working Group.

Peterson noted that the second scheduled presenter, Curtis Dukes (Center for Internet Security—CIS), was unable to join due to a scheduling conflict. Peterson encouraged attendees to review the CIS' prepared materials and emphasized that the CIS is a long-standing and trusted developer of cybersecurity best practices and is actively developing security controls for AI environments. Peterson highlighted the importance of continued engagement on the cybersecurity dimensions of AI, alongside broader data and AI governance discussions.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2026_Spring/WG-Cybersecurity/Spring-Minutes/Minutes-CyberWG032426.docx

Draft: 03/18/26

Cybersecurity (H) Working Group
Virtual Meeting
March 13, 2026

The Cybersecurity (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met March 13, 2026. The following Working Group members participated: Michael Peterson, Chair (VA); Colton Schulz, Vice Chair (ND); Alex Romero and Molly Nollette (AK); Mark Fowler and Richard Fiore (AL); Lori Dreaver Munn (AZ); Wanchin Chou (CT); Tim Li (DE); Matt Kilgallen (GA); Daniel Mathis (IA); C.J. Metcalf (IL); Shane Mead (KS); Kallie Ruggiero Somme (LA); Dmitriy Valekha (MD); Danielle Torres (MI); Gregory Maus (MN); Kim Dobbs (MO); Martin Swanson (NE); Joshua Hilliard (NH); Roger Hayashi (NV); Gille Ann Rabbin (NY); Matt Walsh (OH); Sebastian Conforto (PA); Jamie Adams (WI). Also participating was: Matthew Gendron (RI).

1. Discussed Proposed Edits to the Cybersecurity Event Notification Portal Project Intake Form

Peterson presented a brief summary of the proposed changes made in response to the most recent public exposure period. He noted the inclusion of the first draft of the standard form through which licensees will report cybersecurity event notifications in the portal. Peterson reiterated there is no intention to charge licensees to use the portal. Additional language was added to clarify the System and Organization Controls (SOC) 3 report as requested by industry stakeholders. He reminded the Working Group that SOC exams are performed by licensed Certified Public Accountant (CPA) firms operating under the American Institute of Certified Public Accountants (AICPA) attestation standards

Peterson suggested the next steps for the portal project would be to get the document adopted and, then begin the design and development of the portal through consultation and discussion with stakeholders. The first step in ensuring the portal operates correctly is for regulators to draft the standard form based on Section 6B of the Insurance Data Security Model Law (#668). Peterson said once the NAIC has completed enough development, testing will begin with regulators to ensure it is working correctly. He described that the governance and security procedures could be tested through tabletop exercises using synthetic data to simulate various event types and illustrate the different controls and functions that ensure data is protected. He said that the next steps would require substantial engagement with stakeholders, the industry and regulators, to ensure the portal is developed to deliver the expected functionality, usability, and reduction in complexity

2. Adopted the Centralized Cybersecurity Event Notification Portal Project Document

Dobbs provided a summary of the change management process and explained that many of the comments focused on details such as user access, which is typically provided in different technical requirements documents associated with later parts of the process. She explained that the industry would be invited to provide feedback and participate in collaborative discussions and testing.

Schulz highlighted that, although there is limited direct overlap between the groups, the drafting group for the *Market Conduct Exam Handbook* has begun developing a national response framework for cybersecurity events affecting multiple jurisdictions and entities. He noted that this work assumes the existence of shared reporting and coordination functionality similar to what is being discussed for the portal and encouraged the Working Group to remain mindful of other related workstreams that may touch on or benefit from these capabilities.

Holly Weatherford (Wholesale and Specialty Insurance Association—WSIA) thanked the Working Group for the revised project proposal and expressed appreciation for the collaborative engagement. She stated that the WSIA supports the concept of a licensee-directed cybersecurity event notification portal and recognizes that the revisions reflect movement toward that model. She raised concerns, however, that certain proposal language regarding regulator access could be interpreted to allow broader regulatory discretion. Specifically references to departments being "legally entitled" to access notifications could raise concerns about data governance and legal boundaries. She requested additional clarity and transparency on the intent, scope, and limits of regulator access, and on how access would be structured to align with state law while preserving the licensee-directed framework. She also acknowledged revisions emphasizing reduced compliance costs, noted the removal of references to portal fees and revenue concepts, and asked for ongoing transparency on costs and any future revenue considerations.

Lindsey Stephani (National Association of Mutual Insurance Companies—NAMIC) stated that NAMIC submitted comments and redlines consistent with themes raised throughout the project and thanked leadership for ongoing engagement and discussion. She requested that the meeting minutes reflect that the discussion of the depth and sensitivity of information to be collected will occur later, potentially as part of future technical document discussions. She explained that this request is driven by concerns about concentration risk and concluded her remarks.

Peterson thanked Ms. Stephani and acknowledged her interests and stated there will be multiple future opportunities to discuss those topics. He emphasized that there is no intention to move forward unilaterally or predetermine outcomes, and that questions regarding both the substance and implementation will be addressed as they arise.

LaCosta Wix (AHIP) thanked the Working Group for the opportunity to comment on the recent iteration of the centralized portal intake request form and expressed appreciation for the goal of reducing administrative friction for plans experiencing reportable cybersecurity events. She acknowledged the work completed to date and noted that her organization submitted written comments with more detailed questions and requests for clarification, some of which may be addressed in the revised draft. She emphasized the importance of ensuring robust security and confidentiality protections for the portal given the sensitivity of the information it will house and concluded by thanking the Working Group for the opportunity to comment.

Peterson thanked AHIP and stated that the Working Group appeared aligned and prepared to begin work on the project, with the understanding that outstanding questions and concerns raised in comments would continue to be addressed as the work progresses. He noted his intent to keep those issues in view and work toward resolving the most important items as the project moves forward.

Peterson made a motion, seconded by Dobbs, to adopt the revised centralized cybersecurity event notification portal project document (Attachment Three-A1) as exposed. The motion passed unanimously.

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

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2026_Spring/WG-Cybersecurity/2026 0313Interim-Meeting/Minutes-CyberWG031326.docx

Please check all that apply:	
State Connected	☐
Operational	☐
Regulator Request	☒
Urgent Request *(Requires Immediate EPMO review)*	☐

Name of the Project/Initiative:	Centralized Cybersecurity Event Notification Portal Project
Project Sponsor(s):	Michael Peterson
Person Completing Proposal:	Koty Henry
Submission Date:	03/13/2025

1. **OPPORTUNITY STATEMENT: When answering this question, please describe:**
   - *Why do we need to implement this project?*
   - *What problem are we trying to solve for?*
   - *How do we know this IS a problem to solve for?*
   - *Have we ever done something like this before?*

   The current cybersecurity event notification process required by the Insurance Data Security Model Law #668 (MDL #668) is fragmented and inconsistent across the jurisdictions where it has been passed, adopted, and implemented. This is burdensome for licensees to navigate during a cybersecurity event, adding significant costs to an already expensive process, and increases legal risk due to inconsistent compliance expectations. Additionally, this complexity is a friction point for the industry as legislatures consider the adoption of MDL #668, as licensees must bear additional compliance requirements. Lastly, the Cybersecurity (H) Working Group has charges that would be imperiled by inaction or failure, particularly charges #3 and #8. Without the additional efficiency a central portal would create, developing guidance for cyber events and coordinating any resulting work (Charge #3) would remain overly complicated and slow. Finally, assisting with the passage and implementation of MDL #668 (Charge #8) cannot be reasonably achieved so long as the marginal cost of compliance with a jurisdiction's notification requirement remains high, a problem the central portal will address. In summary, as cybersecurity risks intensify, this lack of a unified, efficient reporting system hinders timely response, complicates compliance, and weakens stakeholder confidence.

   The Cybersecurity (H) Working Group has been working to align the various areas of MDL #668 and the centralized cybersecurity event notification portal is the final piece. Already, guidance documents have been adopted to reduce the compliance burden of industry by aligning the efforts of departments of insurance as they enforce sections 6 and 7: the Cybersecurity Event Response Plan

(CERP), and the Insurance Data Security Model Law Compliance and Enforcement Guide. While both have been adopted and address necessary areas of convergence, the ability to centralize the reporting of cybersecurity events requires technology, not a guide. This project is that technology.

The basic technology underlying the portal, being able to store and receive highly sensitive information while limiting access to only the appropriate users and aligning with well recognized control frameworks and will include clear governance over security, requirements well within the NAIC's capabilities and expertise. This initiative aligns with the CERP adopted in March 2024 and supports the implementation of MDL #668.

2. **PROPOSED SOLUTION: When answering this question, please describe:**
   - *What is the proposed or "ideal" solution?*
   - *What are the intended outcomes?*
   - *Are there any "Hard" Dates to consider?*
   - *Are there any known risks to account for?*

The Cybersecurity (H) Working Group adopted the CERP on March 17, 2024, which guides state insurance regulators on responding to cybersecurity event notifications, required under Section 6 of MDL #668, from licensees. The CERP, however, can only unify the response to a notification by departments, not the underlying requirements faced by licensees to provide notification in the first place. The proposed solution is to develop a secure, centralized portal hosted by the NAIC to receive, manage, and track cybersecurity event notifications from licensed entities in states that have adopted MDL #668.

The portal would be built with a minimum of features, aiming for a high degree of uniformity within a licensee-directed notification system. To accomplish this, a set of notification questions that represent the requirements of all MDL #668 states will be developed into a single, standardized notification form (attachment 1). Data access will be highly limited to only those departments with an adopted version of MDL #668, and the responsibility for selecting those departments will be upon the licensee. Additionally, security concerns should be assuaged by an annual disclosure of a System and Organization Controls Reporting (SOC) 3 report by the NAIC. The SOC 3 report is the public version of the NAIC's SOC 2 Type II that is conducted annually, and their report looks at the Security Trust Services Criteria.

Lastly, as we develop experience additional opportunities may present themselves wherein the portal may be improved. Any such future endeavor will be done in consultation with our stakeholders and interested parties.

Key Features

- Licensee fills out a single, standard notification form, which may be updated as additional facts become known. A draft version of the standard form can be found in attachment 1, where additional details about uploading files can be found.

- Licensee directs notifications by selecting the departments to notify, which may be updated. Secure, role-based access for regulators, providing access only for those who have passed an equivalent to Section 6 of MDL #668.
- Regulators to have the ability to satisfy recordkeeping requirements by downloading completed records.

3. **KEY RESOURCES: When answering this question, please describe:**
   - *What resources/teams are required to deliver the solution?*
   - *What is the projected resource level of estimates for each affected area?*

   The success of a centralized cybersecurity event notification portal relies on the collaboration of internal NAIC teams and regulators, in particular the Cybersecurity (H) Working Group, as well as collaboration with licensees, as warranted.

   Resource needs for this initiative have been identified as follows:
   - *NAIC technical and cybersecurity teams for development and hosting*
   - *Regulatory and legal input to align with state law variations*
   - *Business analysts and project managers to oversee implementation*
   - *Training and support staff for successful rollout and adoption*
   - *Infrastructure Investment (servers/cloud services, licences)*

4. **EXISTING ALTERNATIVES: When answering this question, please describe:**
   - *Do we have an in-house solution in place that COULD meet the existing need?*
   - *Is a new purchase/build absolutely required to meet the project needs?*

   While no single solution currently provides this fully tailored experience, the NAIC has tools and platforms that can enable an efficient and scalable build of such a solution.

5. **VALUE PROPOSITION: When answering this question, please describe:**
   - *Why should the organization invest in this initiative?*
   - *What value will be created by doing this?*
   - *What happens if we DON'T do this?*
   - *If applicable, please indicate the letter committee that adopted this project.*

   The portal is the final piece of a series of initiatives intended to harmonize and align the various cybersecurity requirements found in MDL #668. Once complete, the NAIC membership should be able to more easily pass MDL #668 nationwide, as legislatures will face fewer hurdles from industry as their problems with the law's expansion will have been solved. Further, the streamlined compliance and improved incident response that licensees will achieve will improve operational efficiency by reducing compliance costs and complexity. The portal will allow licensees the ability to submit information about cybersecurity incidents once within the security of the NAIC's systems rather than to multiple states, multiple times, through multiple platforms containing varying levels of security.

Many issues will arise if this project is not pursued. Without a central solution there will continue to be duplicative regulatory efforts to investigate cybersecurity breaches and varying levels of security for submission of cybersecurity breach notifications across departments. Most importantly, failing to align requirements will make it difficult for MDL #668 to be passed in additional jurisdictions, imperiling work on the Cybersecurity (H) Working Group's Charges #3 and #8.

6. **KEY SUCCESS METRICS: When answering this question, please describe:**
   - *What key deliverables will make this project a success?*
   - *How will we know when we are successful?*
   - *What key metrics will be used to define "Doneness"?*
   - *How will we test/validate metrics?*

   The key deliverables necessary to make this project a success would include developing a portal that:
   1. Meets both industry and regulator confidence requirements regarding data security and confidentiality.
   2. Allows licensees to submit cybersecurity event notifications through the portal to those jurisdictions that have adopted a version of Section 6 of MDL #668 that licensees determine should be notified.
   3. Allows each state regulator to receive all information necessary to meet the statutory reporting requirements of their jurisdiction via a standard form.
   4. Allows both regulators and industry participants to satisfy their recordkeeping requirements through secure downloads and robust logging to ensure auditability.
   5. Allows licensees to update the information within the notification, via the portal, as their investigation progresses.
   6. Notifies licensee-selected regulators via email when new information is available for viewing.
   7. Allows licensees to update which regulators who have adopted MDL #668 have access to the cybersecurity event notification, in keeping with their legal responsibilities.

   To measure the success of the proposed centralized portal for cybersecurity event notifications, the following key metrics may be considered:
   1. Number of Cybersecurity Event Notifications: Track the total number of notifications received through the portal to assess adoption and usage.
   2. User Adoption Rate: Monitor the number of licensees and state insurance regulators using the portal and the growth rate of new users. *Maybe consider quantifying the metric by saying something like "**Adoption by at least 5 states in Year 1; goal to scale to 10+ within 2 years**"*
   3. User Satisfaction and Feedback: Collect and analyze feedback from users through incremental surveys to measure satisfaction, system uptime, and identify areas for improvement.

7. **CUSTOMER SEGMENTS: When answering this question, please describe:**
   - *What is the impact to the organization, members, another project or NIPR if this project is not approved?*

- *Who is the customer/member? Who is your audience?*
- *Who are the business owners/stakeholders that will be impacted by this?*
- *Who are the end users?*

Without a central solution there will continue to be duplicative regulatory efforts to investigate cybersecurity breaches and varying levels of security for the submission of cybersecurity breach notifications across departments. Most importantly, failing to align requirements will make it difficult for MDL #668 to be passed in additional jurisdictions, imperiling work on the Cybersecurity (H) Working Group's Charges #3 and #8.

The key stakeholders for this project are members and licensees. Departments of insurance whose legislature has passed a version of Section 6 of MDL #668 will have access to a central repository where every cybersecurity event notification they are legally entitled to is available. This will reduce work for departments as they review and track individual notifications and reduce duplicative and redundant responses. Further, for those states whose legislature has not passed a version of MDL #668 but would like to, the centralized portal will reduce the regulatory burden experienced by licensees as more states adopt.

Licensees will accrue the immediate benefit of a centralized repository as the burden for notifying multiple state departments of insurance will be dramatically reduced through the implementation of a standard form and a push-based, licensee-directed system. Currently, licensees must navigate multiple regulatory schemes for the notification of cybersecurity events, all with their own unique approaches to implementation. This fragmentation has led to a slow and ultimately expensive process for licensees.

8. **COST STRUCTURE: When answering this question, please describe:**
   - *What known costs are associated with the project (i.e., Software, Hardware costs, etc.)*
   - *Are there any 3rd party vendor costs to consider?*

Staffing Options & Estimate:

Below are Assumptions and Staffing Options/Estimates for the Centralized Cybersecurity Event Notification Portal Project EPMO proposal dated 2/11/26. Note that the timing of this effort could affect the quoted amounts and timelines based on staff availability.

Assumptions:

- Deliverable will be a single solution for all jurisdictions.
- Prototype using Appian and Design review with Working Group is completed prior to project approval by EPMO.
- Team is comprised of Product Owner, 3 Software Engineers and 1 Software Quality Engineer
- Prototype is for discussion purposes; the team will meet UI/UX and Appian guidance for the development work.
- Option one assumes the team is working 75% of the time on this project with the rest of the time allocated to other work to support existing applications.

The following phases are recommended:

Phase	Key Activities
Project Preparation Phase	Training (Option 2), planning, understanding project, refinement of work.
Development (MVP)	Build core features: intake form, role-based access (admin, company and regulator, audit trail, notifications). Reuse components and tables from UCAA and SERFF where appropriate.
Testing & Validation	Functional testing, automation testing, Dynatrace Synthetic, security validation, UAT with early adopters.
Pilot Rollout (5–10 states)	Controlled launch, feedback loop, refinements.
Full Rollout & Support Setup	Training, documentation, help desk, onboarding additional states.

- H Committee staff support will provide ongoing administrative support.
- On-going staff considerations also include .25 ITG FTE for maintenance and support post-release.

Staffing Options/Estimates

1. **A dedicated ITG delivery team with existing Appian development experience and no outside help.** This team will not need startup and training time/costs; however, this option may not be feasible based on anticipated workloads.

Cost: $0 consulting costs – NAIC internal labor only
Duration: 7.5-8 months

2. **An ITG delivery team with no Appian development experience and the assistance of one full-time NAIC Appian Software Engineer.** This approach enables the delivery team to complete current tasks within an extended duration. Training and startup time allocated is included for a team new to Appian. The mentor's team will have reduced capacity for the duration of the project.

Cost: $16,500 instructor led training and certification for 3 engineers, the team will be unavailable for other work.
Duration: 9.5-10 months

3. **Outsourced to a professional services consulting group, with oversight of NAIC staff.**

Cost: $2.1M consulting costs, and reduced capacity of NAIC staff working with outside firm
Duration: 7.5-8 months

9. **RISK MITIGATION: What risks should you mitigate to make the project successful? When answering this question, please describe known risk factors associated with implementing this project, such as:**
    - *Are there risks to achieving a high adoption?*
    - *Is this a new effort we've never done before?*
    - *Do we need to acquire innovative technology to implement?*

The NAIC is exceptionally well positioned to construct and administer the portal, and it fits well into its existing expertise. Accepting data, even highly sensitive and confidential data, is something NAIC does well and has done for a long time across many domains. However, some general risks remain, which are discussed below.

Risk: Stakeholders lack a method by which to understand the current security posture of the portal.

Mitigation: NAIC should make available, annually, a SOC 3 report for public review by licensees and other interested parties. The SOC 3 is the public version of a SOC 2, an industry-recognized and respected third-party assurance report, which preserves the sensitive security information of the NAIC.

Risk: Access and confidentiality protections for licensees.

Mitigation: Access to the portal will be based on whether a department's legislature has passed a version of Section 6 of MDL #668. The licensee, utilizing a push-based system, will select the departments to receive their notification as their legal responsibility requires. Like the form, the departments able to view the notification can be updated by the licensee. The NAIC will have limited access to enable support only, and will mirror the access they retain for other, highly sensitive information like RBC data, ORSA reports, and exam information.

Risk: Difficulty in tracking changes and updates to a notification by departments.

Mitigation: Given the simplicity of the design of the portal, with licensee-directed notifications, this difficulty is best addressed through a robust logging capability. This will provide the necessary insight for departments to understand how the notification has been changed and updated over time.

Risk: The underlying data increases in its sensitivity, which may result in higher cybersecurity risk to the licensee cybersecurity event information.

Mitigation: If highly sensitive information begins to be included in the portal, then cybersecurity risk becomes elevated in importance. To handle the prospective risk of elevated cybersecurity, a SOC3 report should be provided annually, which will ensure stakeholder clarity that highly sensitive information is adequately secured by NAIC.

Risk: Using the portal is difficult and causes problems for departments.

Mitigation: Clear instructions will be made available and training, if necessary, will be developed and offered.

While other risks may be present, all the risks found insofar have been found to have mitigation strategies that are acceptable to stakeholders.

10. **Member Support:** When answering this question, please document the members who are in support of this initiative.

Ensuring the alignment of the majority of members is crucial for the success of any initiative. The new EPMO project process is structured to foster collaboration and build consensus through a transparent, phased approach:

- The proposal will first be presented to the Cybersecurity (H) Working Group, providing a focused forum for subject matter experts and key stakeholders to evaluate the initiative, raise concerns, and offer recommendations. This early engagement ensures technical and operational considerations are addressed before moving forward.
- Following the Working Group's input, the proposal will advance to the Innovation, Cybersecurity, and Technology (H) Committee for broader member review. This step allows for strategic alignment across the organization to ensure that all members have an opportunity to provide feedback and influence the direction of the project.

This transparent, consensus-focused approach will provide the necessary alignment among all stakeholders to allow for member support to build organically.

11. **PROJECT DEPENDENCIES: Is this project dependent on other projects or initiatives? If yes, please list.**

No, this project does not depend on other projects or initiatives.

12. **HARD DEADLINES: Is there a deadline driving this project? ☐YES ☒NO If yes, what is it?**

13. **REVENUE STREAMS/SOURCES: When answering this question, please describe:**

- **Will this effort generate additional revenue or cost money to implement? ☐YES ☒NO**

Revenue generation from non-licensees may be explored in later phases. The current proposal is not predicated upon the recovery of costs from licensees.

- **If so, what is the revenue projection?**

14. Could an additional fee be charged to recoup costs and/or are there future budgetary cost savings? ☐YES ☒NO

15. Will NIPR share costs? ☐YES ☒ NO If yes, indicate your rationale and list the NIPR contact.

16. Provide high-level estimates for the initial and future costs associated with this project.

➢ **Please insert additional rows if needed.**

Software Licenses and/or Subscriptions – Type *(include maintenance on separate line)*	Number Requested	Individual Cost	Starting Month and Year	Length of Initial Term	% Allocated to NIPR
				3-Year	
		$			
TOTAL		$			

Hardware Purchases – Type *(include maintenance on separate line)*	Number Requested	Individual Cost	Starting Month and Year	Length of Initial Term *(maintenance only)*	% Allocated to NIPR
		$			
		$			
TOTAL		$			

Consulting – Staff Aug. Position Title (each requested consultant on its own line)	Proposed Hourly Rate or Fixed Engagement	Estimated Hours for Contract Term	Length of Contract Term	Starting Month and Year	% Allocated to NIPR
	$				
	$				
TOTAL	$				

Consulting – Prof. Services Position Title (each requested consultant on its own line)	Proposed Hourly Rate or Fixed Engagement	Estimated Hours for Contract Term	Length of Contract Term	Starting Month and Year	% Allocated to NIPR
TOTAL					

Training / Conferences / Certifications - Type	Number Requested	Individual Cost	Month and Year Attending or Start of Subscription	Is this an annual subscription. (Yes / No)	% Allocated to NIPR
		$			
		$			
TOTAL		$			

Travel – Purpose and Location if Known	Number Individuals Traveling	Number of Nights per Individual	Individual Cost from Current Travel Matrix	Month and Year of Travel
			$	
			$	
TOTAL			$	

New Headcount Requests – Job Description Title	Number Requested	Proposed Salary	Starting Month and Year
		$	
		$	
TOTAL		$	

17. What assumptions have been factored into the project estimates?

- It is assumed that the number of workforce identities will remain consistent at 1,000 over the 3-year term. While this number is currently accurate, the NAIC may experience growth.
- The estimates assume that the implementation and integration of the Identity and Access Management (IAM) tool with existing systems (Active Directory, Okta, eDirectory, Workday) will be completed within the planned timeline without significant delays.
- It is assumed that internal teams, including the IAM team and identity teams, will be available and have the necessary expertise to support the implementation and integration efforts.

- The estimates assume that the selected IAM tool will be compatible with the NAIC's existing identity systems and will not require significant additional customization or development.
- The cost estimates do not include a managed service offering for ongoing support. The NAIC may choose to purchase this offering in the future.

18. Please indicate the staff resources needed for this project in the table below.
Please insert additional rows if needed. Only technical hours will be tracked for the project.
Replace 0 with numbers. Highlight Total Number, Right click, Update field.

Internal Resources	Area/Team	Number/Type (Ex: 2-Analysts, 3-SE)	Total Estimated Hours

19. What is your confidence level in the above estimates? *Low estimates will not be considered by the EPMO*.

☐ **HIGH**
Please comment:

☐ **MEDIUM**
Please comment:

20. Does the project include any of the following: PII/MNPI/other confidential information, attachments or ad-hoc data access? ☐**YES** ☐**NO**
If yes, please provide details regarding the confidential information, size, and number of attachments/retention period or ad-hoc data access needs.

-
-
-
-

For EPMO use only – do not fill out.

Account Description	Account Code / Dept	Total Expense for Initial Budget Year	Estimated Expenses for Following Year	Total Capital for Item (if Applicable)	Starting Month of Amortization or Depreciation	Length of Term	% Allocated to NIPR
		$	$	$			
		$	$	$			
Totals for EPMO spreadsheet		**$**	**$**	**$**			
Totals for NAIC		**$**	**$**	**$**			
Totals for NIPR		**$**	**$**	**$**			