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

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		**$**	**$**	**$**			

The Confidential Cybersecurity Event Notification Portal

An overview of the project

Project Development History

- The Cybersecurity Event Notification Portal Project has been carefully developed to arrive at the current consensus:
  - The Cybersecurity (H) Working Group began discussing a centralized solution in early 2024, and at the 2024 Fall National Meeting a motion to explore the portal's creation was adopted after hearing from stakeholders.
  - The project proposal was presented at the 2025 Fall NM, where additional comments were received. Those were incorporated into a new version, which received another public comment period beginning in February 2026.
  - The final version of the project documentation was adopted by working group in March 2026, after the last set of stakeholder comments were incorporated.
- The portal's design encourages broader passage of the Insurance Data Security Model Law #668 by compounding the compliance cost reduction with each additional jurisdiction that passes the model law.

Insurance Data Security Model Law #668

- The Insurance Data Security Model Law #668 (MDL-668) requires that licensees notify the Commissioner(s) of Insurance of any qualifying cybersecurity event.
- As state legislatures passed their own versions of MDL-668 the number of commissioners entitled to a cybersecurity event notification grew, imposing a steadily increasing regulatory burden on licensees.
- To reduce the existing and future fragmentation across state departments of insurance and reduce cost and complexity to licensees, a project to centralize the notification of cybersecurity events has been adopted by the Cybersecurity (H) Working Group.

Cybersecurity Event Notification Portal

- The project documentation adopted by the working group to build details a licensee directed (controlled) portal for the notification of cybersecurity events to those departments whose legislatures have passed a version of Section 6B (Notifications).
- The portal will use a standard notification form that blends the states various requirements into a single form for licensees, a draft of which was included in the project documentation.
- Because of the confidential nature of details surrounding cybersecurity events, both the security and confidentiality of the underlying data will be demonstrated by an annual SOC 3 report.

Next Steps & Development

- The approval of the project proposal marks the beginning of a substantial project that will require additional input from stakeholders.
- Testing and a robust tabletop demonstration utilizing synthetic data would be opportunities for stakeholders to confirm that the project is being developed as described, and to offer input on development.
- Once the project is complete and stakeholders are comfortable with the design and operation of the portal, it will be deployed for use by licensees and departments of insurance.

Summary

- The Cybersecurity Event Notification Portal seeks to reduce current and future compliance cost and complexity associated with the Insurance Data Security Model Law #668.
- The Portal will use a standard notification form that blends all the requirements found in the various versions of MDL-668 passed by state legislatures, to further reduce fragmentation and complexity.
- While the Cybersecurity (H) Working Group has adopted the project plan, additional work and input from stakeholders will be necessary as the project moves forward to ensure all needs are adequately met.