

March 9, 2026

Koty Henry
Cybersecurity Policy Advisor, P&C Regulatory Services
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106-2197

By Email to: Koty Henry at khenry@NAIC.org.

Re: NAIC Cybersecurity (H) Working Group Exposure of Cybersecurity Event Notification Portal Intake Request Form

Dear Mr. Henry:

On behalf of AHIP, thank you for the opportunity to provide feedback on the proposed Cybersecurity Event Notification Portal (“Portal”) Intake Request Form (“Form”).

We understand that the Working Group’s objective in developing a cybersecurity event notification portal is to create a unified and efficient reporting mechanism for qualifying events. While we are generally supportive of that effort, we offer the following questions and recommendations for consideration prior to finalizing the Portal.

Scope & State Variability:

- Confirm the Portal is limited to MDL #668 Section 6 notifications and dynamically adapts to each state’s statutory elements/timelines. Participation and acceptable alternatives should be transparent by jurisdiction.
- Confirm that states will all accept the same information from reporting entities. Absent uniform acceptance of submitted information, duplicative regulatory requirements and inconsistent security standards may persist.

Access Roles and Security:

- Stakeholders need clear information regarding the access roles to be created and who is authorized to access the Portal and access submitted data; this includes individuals within state insurance departments, NAIC personnel, and any third-party vendor(s) supporting the platform. Access rights should be consistent with established data governance frameworks such as HIPAA.

March 6, 2026

NAIC Cybersecurity (H) Working Group
NAIC Central Office
1100 Walnut Street
Suite 1500
Kansas City, MO 64106
Via email: khenry@naic.org

RE: Updated Cybersecurity Event Notification Portal Project Intake Form

Chair Peterson and Members of the Cybersecurity Working Group:

Thank you for the opportunity to provide comments on the updated draft Cybersecurity Event Notification Portal Project Intake Form. APCIA appreciates the Working Group's continued efforts to strengthen cybersecurity event reporting and improve coordination among state regulators.

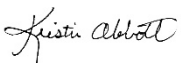
APCIA remains supportive of the overall concept of a centralized Cybersecurity Event Notification Portal. A single, secure submission point has the potential to reduce administrative burden, promote consistency across jurisdictions, and streamline the reporting process during time-sensitive cyber events. As we have previously emphasized, it is essential that such a portal be secure, that all data be kept confidential, and that any submitted notices be shared only with the intended regulatory bodies. Ensuring strong protections around data access, transmission, storage, and sharing will be foundational to the Portal's success and stakeholder trust.

We are encouraged by the direction of this initiative and are comfortable with the project continuing to move forward. At this stage, our comments remain consistent with the feedback we previously provided. As before, APCIA's support is grounded in the understanding that stakeholders will have a meaningful opportunity to review and evaluate an initial beta version of the Portal once it is developed. A demonstration or test environment, paired with an opportunity to offer targeted feedback, will be critical to assessing practical functionality, usability, and alignment with regulatory and industry needs. We look forward to providing more detailed, substantive feedback at that time.

We also continue to encourage periodic check-ins throughout the development process. Regular touchpoints will help ensure the project remains informed by real-world considerations and will allow stakeholders to engage constructively as the Portal takes shape.

APCIA appreciates the opportunity to remain engaged and supports continued progress on this initiative.

Thank you,



Kristin Abbott

- Will role-based access requirements extend beyond regulators?

SLAs & Resilience:

- Publish availability metrics (including RTO and RPO), incident-response services levels, and 24×7 support expectations for Portal, and conduct joint tabletop and failover exercises prior to broad adoption and implementation.

APIs & Interoperability:

- Provide standard schemas and secure application programming interfaces (APIs) for system-to-system submissions, updates and multi-state filings, while accommodating state-specific requirements.

Governance, Liability & Cost:

- Clarify liability in the event of a Portal security incident, establish change-control for form or schema updates, and outline any cost-recovery model, if any, to ensure predictability.

NAIC SOC3 Report

- Clarify which trust service criteria will be tested - security, availability, integrity, confidentiality, and/or privacy.
- Given the sensitivity of the data and the critical function of the Portal, all five trust service criteria should be tested.

Thank you for the opportunity to submit these important considerations. We look forward to continued collaboration through the development of a notification Portal that will serve both regulators and submitters.

Sincerely,

LaCosta Wix
AHIP Senior Regulatory Counsel, State Affairs and Policy

lwix@ahip.org
504-579-6287

Cc: Miranda Motter, Senior Vice President, State Government Affairs and Policy

March 6, 2026

Michael Peterson (VA), Chair
NAIC Cybersecurity (H) Working Group
c/o Koty Henry, NAIC Cybersecurity Policy Advisor, P&C Regulatory Services
via email khenry@naic.org

Re: Cybersecurity (H) Working Group Centralized Cybersecurity Event Notification Portal Project v.3

Chair Peterson and Members of the Working Group:

On behalf of the National Association of Mutual Insurance Companies (NAMIC)¹, we are writing in response to the Cybersecurity Working Group’s efforts toward a centralized reporting portal, and version three of the corresponding project proposal.

While NAMIC supports and similarly sees a need for efficiency in the event reporting process, we have outstanding concerns with the Working Group’s reporting portal as proposed for the following reasons:

- **[1] The reporting efficiency to be gained is not significant;**
- **[2] Promises of security by the NAIC are not enough to assuage the concentration risk concern;**
- **[3] There are alternative projects the Working Group could pursue in place of the portal.**

We elaborate on these outstanding concerns below. Attached with this letter is a document with suggested redlines to the project proposal request, and **we call specific attention to limiting the level of information and detail that would be put into the portal. Limiting the level of data and detail put into the portal would lessen our concentration risk concern.**

SUBSTANTIVE COMMENTS

[1] The Reporting Efficiency to be Gained is not Significant

While the portal is creating one spot to submit reports, reporting structure and substance still differs across states; it may solve the “one-to-many” problem for Model # 668 states, but will not solve for states that have not adopted the Model (or adopted variations), nor solve for state

¹ The National Association of Mutual Insurance Companies (NAMIC) is the foremost trade association representing the property/casualty insurance industry. Serving more than 1,300 member companies—including local and regional insurers as well as some of the nation’s largest carriers—NAMIC members collectively write \$467 billion in annual premiums, representing 61% of the homeowners and 53% of the automobile insurance markets. For more than 130 years, NAMIC has been the leading voice advancing public policy solutions and regulatory frameworks that promote a strong, competitive market and protect our members and their policyholders.



attorney general reporting (which comprise the bulk of insurer breach notification responsibilities).

Model # 668 was adopted in 2017, and only 28 jurisdictions have adopted the Model to date. Of those 28 jurisdictions that have adopted the Model, **there are substantive differences in the adopted model, and (most importantly for the portal) there are differences in the requirements for notification of a cybersecurity event.** On timing of the notification, a majority of the adopted states require “as promptly as possible,” (but no later than three business days). Yet, other states allow for five to ten business days², and some do not include “as promptly as possible” language.³ In terms of reporting criteria, all states except Alaska, Maine, and South Carolina, depart from the Model considerably on what constitutes a “cybersecurity event” about which a licensee must notify the commissioner. To illustrate this, seventeen states **alter** the domicile notification criteria that the event also have a reasonable likelihood of materially harming a consumer residing in the state, or any material part of the normal operation of a licensee, for the notification requirements to be triggered.⁴

In addition to differences among Model states and what triggers the reporting itself, there are differences among Model states in the information to be provided in the cyber event notification, including some states omitting the requirement to include “as much of the following information as possible,” amending the requirement to provide as much of the information as “reasonably” possible, and differences in the continuing obligation to update and supplement initial notifications.⁵ **Put another way, even with the potential for one portal to submit notifications through, the notifications themselves will still have differences, thereby discounting the amount of efficiency gained.** These are all differences among merely the Model states themselves, and don’t include the differences in reporting among non-Model states.

Further, the majority of an insurer’s breach and cyber reporting obligations are to state attorneys general⁶; reporting to state departments of insurance represents a small part of breach reporting obligations. Having one location, or one portal, to submit insurance specific cyber event reporting will not eliminate the need to report to state attorneys general, and therefore will not be a significant efficiency gain for this reason alone. This fact is also notwithstanding the differing reporting requirements among state insurance departments

² See, e.g., MO Bulletin 2023-04 (2023) (as soon as practicable, but no later than 10 days); Minn. Stat. Ann. s. 60A.9853 (2021) (without unreasonable delay but in no event later than five business days); 40 PA C.S. s. 4518 (2023) (as promptly as possible, but in no event later than five business days).

³ See, e.g., Iowa Code Ann. S. 507F.7 (2020); N.H. Rev. Stat. Ann. S. 420-P:6 (2019).

⁴ See, e.g., Ala. Code s. 27-62-6 (2019); Conn. Gen. Stat. Ann. S. 38a-38 (2020); 215 Ill. Comp. Stat. Ann. 215 (2024); Id. Code Ann. S. 27-2-27-21 (2020); Ky. Rev. Stat. s. 304.3-760 (2022); La. Rev. Stat. s. 22:2506 (2020); Mich. Comp. Laws s. 500.559 (2018); Minn. Stat. Ann. s. 60A.9853 (2021); Miss. Code Ann. s. 83-5-811 (2019); N.H. Rev. Stat. Ann. s. 4200P:6 (2019); Ohio Rev. Code Ann. s. 3965.04 (2018); Okla. Stat. tit. 36 s. 675 (2024); 40 Pa. C.S. s. 4518 (2023); Tenn. Code. Ann. s. 56-2-1006 (2021); Wis. Stat. Ann. s. 601.954 (2021).

⁵ See, e.g., Conn. Gen. Stat. Ann. S. 38a-38 (2020); Iowa Code Ann. S. 507F.7 (2020); Ky. Rev. Stat. s. 304.3-760 (2022); 40 Pa. C.S. s. 4518 (2023); Tenn. Code. Ann. s. 56-2-1006 (2021); Wis. Stat. Ann. s. 601.954 (2021).

⁶ See, US State Data Breach Notification Chart, IAPP, <https://iapp.org/resources/article/state-data-breach-notification-chart> (chart providing references to and information on US state and territory data breach notification laws).



themselves. **Placing emphasis instead on establishing a consistent reporting format across states would better solve for multi-regulator reporting**, rather than focusing efforts on creating one portal.

As such, the NAIC would be creating a risk not worth the reward – the portal would create a potentially substantial concentration risk, while not achieving much in the way of reporting efficiency.

[2] Promises of Security by the NAIC are not Enough to Assuage the Concentration Risk Concern

While the Working Group has referenced the NAIC’s experience housing sensitive information, cyber event reporting information is different than what the NAIC has housed in the past. Whereas a breach of information that NAIC currently has would lead to confidential information access, a breach of the centralized reporting portal would give a cyber-criminal information on insurer *system* access.

In response to NAMIC’s concern that the centralized reporting portal creates a concentration risk (by centralizing breach response measures and information on the entire industry in one location), the Working Group has repeatedly stated that: 1) The NAIC has experience in housing sensitive information; 2) The portal will be more secure than state processes today; and 3) The NAIC will provide a SOC 3 report annually, to assuage industry security concerns.

Cybersecurity event information is different from information that the NAIC currently houses; if a cyber-criminal gains access to the information called for in Model # 668 for a cyber event report, the NAIC has now given that cyber-criminal information on how to infiltrate insurer systems and take companies offline. This is different than purely confidential information access; this is system access.

While state insurance departments already have this cyber risk to some degree, we do not believe that the NAIC should knowingly create a greater degree of that risk by creating the same type of attack opportunity, and pooling all of the cyber event notifications into one location. The NAIC has also further alleged that some states obtain this information via lesser secure avenues; though, this is not every state department’s experience. As we explain in a later section of this letter, the Working Group could pursue guidance for states on security best practices, rather than creating this portal.

SOC 3 (a public view of SOC 2) reports do not assuage industry concerns of *concentration risk*; good security practices are simply table stakes. Good security practices alone do not solve for the risk of housing cyber information in one location – data minimization efforts are key to solve for concentration risk. Good security practices also do not solve for new attack strategies that cyber-criminals continue to devise. Further, SOC 2 and 3 certifications or reports only look at operational excellence and do not include a robust substantive security focus. The reports also vary greatly depending on who performed the review; so the report is only as good as the auditor that fashioned it.



[3] There are Alternative Projects the Working Group Could Pursue in Place of the Portal

If reporting efficiency is top of mind, the Working Group could focus its efforts on consistent Model # 668 adoption, or amendments to Model # 668 to allow for lead-state reporting. If security in reporting is top of mind for the Working Group, it could focus on devising guidance for state insurance departments on best practices for collecting cyber event reporting information, or limit the amount of information and level of detail into the portal to reduce concentration risk.

[4] Commentary on Portal Project Itself

Notwithstanding our comments above, and consistent with concerns we have raised throughout the cyber portal discussions, we have included as an attachment suggested redlines to the current project proposal request through which we've highlighted important themes and areas of focus.

Data Minimization and Limiting Detail in the Portal

To the extent the project moves forward, NAMIC strongly believes that the NAIC should limit the amount of information and level of detail put into the portal. **Limiting the level of data or detail put into the portal, especially relative to sensitive substantive information like is called for in subs. (10) and (11) in Section 6B of Model 668 would lessen the concentration risk concern.**

Confidentiality and Access Permissions

Confidentiality and limiting access permissions will be of utmost importance given the sensitive nature of the data the portal would house. The project plan currently limits access to states that have adopted Model 668, but NAMIC requests that data access be limited further to only those departments to which a licensee has directed the cyber event notification under the requirements of Model # 668. States in which a licensee has not experienced a cyber event and necessitated a report should not have access to said reports for confidentiality purposes. NAMIC also requests that the NAIC detail the access permissions and justifications for the access and permissions of NAIC staff.

Cost and Revenue Streams

The project plan currently states that revenue generation capability may be explored later. NAMIC requests that the NAIC provide detail on: 1) Whether licensees will be required to use the portal; and 2) Whether there will be any initial costs to companies to use the portal, or costs and fees that are contemplated after the portal's establishment.

IN SUMMARY

We close by again emphasizing our agreement that current cyber event reporting lacks efficiency and security across the board, but also highlighting our concern that the current portal project as proposed does not fully achieve efficiency, and creates additional security risk itself. In this vein, we've proposed potential



alternatives to the portal altogether, as well as considerations for the portal itself to lessen concentration risk concern and confidentiality concerns. NAMIC looks forward to continuing our work with the Working Group to arrive at solutions that protect and benefit all stakeholders.

Sincerely,

Lindsey Stephani

Lindsey Stephani
Policy Vice President – Data Science, Artificial Intelligence, and Cybersecurity
NAMIC

NAMIC Suggested Redlines and Comments

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: 05/26/2025

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 and can add significant costs to an already expensive process. Additionally, this complexity is a friction point for industry as legislatures consider 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 work that results (Charge #3) would remain excessively 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

NAMIC Suggested Redlines and Comments

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, is 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 provides guidance to 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. Data access will be highly limited to only those departments with an adopted version of MDL #668 ~~that a licensee has directed the information be sent to under the requirements of MDL # 668. The NAIC will provide an annual disclosure of a system and Organization Controls Reporting (SOC) 3 report that has also undergone an independent review or assessment. As part of the project, the NAIC will also develop and share its plans with interested regulators and parties of how it expects to report and handle any cyber events it itself experiences with the portal, and the responsibility for selecting those departments will be upon the licensee. Lastly, security concerns should be assuaged by an annual disclosure of a System and Organization Controls Reporting (SOC) 3 report by the NAIC.~~

Key Features

- Licensee fills out single, standard notification form, providing high-level or categorical type answers to the most sensitive areas of information, which may be updated as additional facts become known.
- Licensee directs notifications by selecting the departments to notify, which may be updated. Only those state departments a licensee directs will have access to the information submitted.

Commented [LS1]: To the extent the project moves forward, NAMIC requests that the notification questions/form only require simple or categorical type answers to the Model 668, Section 6.B, subs. (10) and (11). Because these Model 668 sections call for highly sensitive details about a cyber event, centralizing this information at a deep level of detail creates a potentially substantial concentration risk.

NAMIC Suggested Redlines and Comments

- Secure, role-based access for regulators, providing access only for those who have ~~passed an equivalent to Section 6 of MDL #668~~. ~~been sent a notification by a licensee through the portal.~~
- ~~Regulators to have the ability to satisfy recordkeeping requirements by downloading completed records.~~
- ~~[Description of access and permissions of NAIC staff]~~

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. The NAIC commits to a transparent procurement and selection process for a vendor to support the 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

Commented [LS2]: NAMIC requests detail around the access and permissions (as well as justifications for the access and permissions) of NAIC staff.

NAMIC Suggested Redlines and Comments

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"*

NAMIC Suggested Redlines and Comments

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 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 are available. This will reduce work for departments as they review and track individual notifications and reduce duplicative and redundant response. 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:

NAIC's Enterprise Project Management Office (EPMO) is currently working to update the estimates, and they will be made available as soon as they are produced.

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

NAMIC Suggested Redlines and Comments

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 with an independent review or assessment 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. The NAIC acknowledges that a SOC 3 report does not solve the issue of centralizing a high volume of sensitive information in one location, but that the SOC 3 report only looks at security operational excellence.

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 and whether a licensee has pushed a notification to a department. 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, and the pooling of that information on the entire industry in one location which may result in results in higher cybersecurity risk to licensee cybersecurity event information.

Mitigation: If highly sensitive information begins to be included in the portal, then cybersecurity risk becomes elevated in importance. The only way to truly mitigate a

Commented [LS3]: NAMIC requests detail on which NAIC staff will have access, and more detail on what the access and permissions look like.

NAMIC Suggested Redlines and Comments

~~concentration risk issue is through data minimization, which may start to be solved through requiring a lower level of detail of highly sensitive information be put into the portal. 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. A SOC 3 report with an independent review or assessment will be provided annually for public review by licensees and other interested parties. The NAIC acknowledges that a SOC 3 report does not solve the issue of centralizing a high volume of sensitive information in one location, but that the SOC 3 report only looks at security operational excellence.~~

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. Training on good cybersecurity practices when accessing and using the portal will also be provided to departments.

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

NAMIC Suggested Redlines and Comments

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 capability may be explored later.

- 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 <i>(include maintenance on separate line)</i>	Number Requested	Individual Cost	Starting Month and Year	Length of Initial Term	% Allocated to NIPR
				3-Year	
		\$			
TOTAL		\$			

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

Commented [LS4]: NAMIC requests detail on: 1) Whether licensees will be required to use the portal; and 2) What the NAIC intends with this sentence relative to potential fees to use the portal.

NAMIC Suggested Redlines and Comments

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			\$	

NAMIC Suggested Redlines and Comments

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:

NAMIC Suggested Redlines and Comments

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.

-
-
-
-

Commented [LS5]: The portal project would involve confidential information, so NAMIC requests the NAIC fill out this section.

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		\$	\$	\$			

Northwestern Mutual Suggested Redlines and Comments

Please check all that apply:

State Connected

Operational

Regulator Request

Urgent Request

(Requires Immediate FPMO)

Name of the Project/Initiative: Centralized Cybersecurity Event Notification Portal Project
Project Sponsor(s): Michael Peterson
Person Completing Proposal: Koty Henry
Submission Date: 05/26/2025

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 and can add significant costs to an already expensive process as well as additional legal risk. Additionally, this complexity is a friction point for industry as legislatures consider 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 work that results (Charge #3) would remain excessively 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.

Commented [CM1]: May want to include increased legal risk due to the current fragmented system.

Northwestern Mutual Suggested Redlines and Comments

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.

Commented [CM2]: This aligns with NIST's control catalog approach

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 provides guidance to 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. 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. Lastly, security concerns should be assuaged by an annual disclosure of a **System and Organization Controls Reporting (SOC) 3 report** by the NAIC.

Commented [CM3]: How will submitted information be treated for confidentiality purposes? For example, permitted uses, disclosure limitations, and how the portal approach will preserve protections comparable to current regulator submission channels.

Key Features

- Licensee fills out single, standard notification form, which may be **updated** as additional facts become known.
- Licensee directs notifications by selecting the departments to notify, which may be updated.

Commented [CM4]: SOC 3 is helpful. Will any other assurance artifacts be available to stakeholders such as a scope statement, independent testing summaries, and any other documents/assurance?

Commented [CM5]: Will the updates maintain prior versions including timestamps and change history?

Northwestern Mutual Suggested Redlines and Comments

- 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.

Commented [CM6]: Consider adding another bullet that lists acknowledgement/receipt indicators (e.g., when a notified regulator has accessed the submission or an update), which can reduce duplicative follow-ups during high-pressure incidents.

Commented [CM7]: Please consider specifying that licensees can export submitted information in structured, machine-readable formats (in addition to human-readable downloads) to support internal audits, compliance documentation, and efficient follow-up.

Commented [CM8]: To strengthen credibility, consider committing to tracking and reporting (in aggregate) measurable outcomes such as reductions in duplicative submissions, follow-up requests, and time-to-complete notification workflows.

Northwestern Mutual Suggested Redlines and Comments

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.

Northwestern Mutual Suggested Redlines and Comments

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 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 are available. This will reduce work for departments as they review and track individual notifications and reduce duplicative and redundant response. 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.

Commented [CM9]: It may be helpful to explicitly address how the portal reduces burden for small and mid-sized licensees (e.g., simplified workflows, clear guidance, and minimized duplicative requests), not only large carriers.

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:

NAIC's Enterprise Project Management Office (EPMO) is currently working to update the estimates, and they will be made available as soon as they are produced.

9. RISK MITIGATION: What risks should you mitigate to make the project successful? When answering this question, please describe known risk factors associated with

Northwestern Mutual Suggested Redlines and Comments

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 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.

Commented [CM10]: In addition to SOC disclosure, consider committing to periodic, risk-based security and governance assessments with a stakeholder-facing summary of scope and high-level results.

Commented [CM11]: Consider explicitly addressing the risk that a centralized repository could be perceived as a single authoritative source for incident information, and describing safeguards to prevent its use as a shortcut for third-party access requests. Clarifying intended use and access boundaries upfront would help preserve existing confidentiality expectations.

Commented [CM12]: Please clarify the ongoing support model (e.g., help desk coverage, incident-time escalation path, FAQs/training materials, and service expectations), as these elements are critical during active cybersecurity events. Also, suggest clarifying controls around staff access with least privilege expectations.

Commented [CM13]: May be helpful to specify that logs are protected from tampering, retain adequate detail for investigations, and use consistent time synchronization to support cross-jurisdiction incident analysis

Northwestern Mutual Suggested Redlines and Comments

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.

Commented [CM14]: Perhaps a commitment to usability and accessibility testing, recognizing that users will operate under time pressure and may include a wide range of technical sophistication.

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:

Northwestern Mutual Suggested Redlines and Comments

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

Revenue generation capability may be explored later.

- 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 <i>(include maintenance on separate line)</i>	Number Requested	Individual Cost	Starting Month and Year	Length of Initial Term	% Allocated to NIPR
				3-Year	
		\$			
TOTAL		\$			

Hardware Purchases – Type <i>(include maintenance on separate line)</i>	Number Requested	Individual Cost	Starting Month and Year	Length of Initial Term <i>(maintenance only)</i>	% 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	\$				

Northwestern Mutual Suggested Redlines and Comments

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,

Northwestern Mutual Suggested Redlines and Comments

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:

Northwestern Mutual Suggested Redlines and Comments

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		\$	\$	\$			



EPMO Project Proposal Request Form

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: 05/26/2025

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 and can add significant costs to an already expensive process. 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 ~~work that results (Charge #3) would remain excessively~~ 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.



EPMO Project Proposal Request Form

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, is 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 ~~provides guidance to~~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. 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. Lastly, security concerns should be assuaged by an annual disclosure of a System and Organization Controls Reporting (SOC) 3 report by the NAIC.

Key Features

- Licensee fills out a single, standard notification form, which may be updated as additional facts become known.
- 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:



EPMO Project Proposal Request Form

- *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



EPMO Project Proposal Request Form

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~~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?*



EPMO Project Proposal Request Form

- *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 are-is available. This will reduce work for departments as they review and track individual notifications and reduce duplicative and redundant responseresponses. 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|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:

NAIC's Enterprise Project Management Office (EPMO) is currently working to update the estimates, and they will be made available as soon as they are produced.

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?*



EPMO Project Proposal Request Form

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~~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~~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.



EPMO Project Proposal Request Form

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 capability may be explored later.

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

14. Could an additional fee be charged to recoup costs, and/or are there future budgetary cost



EPMO Project Proposal Request Form

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 <i>(include maintenance on separate line)</i>	Number Requested	Individual Cost	Starting Month and Year	Length of Initial Term	% Allocated to NIPR
				3-Year	
		\$			
TOTAL		\$			

Hardware Purchases – Type <i>(include maintenance on separate line)</i>	Number Requested	Individual Cost	Starting Month and Year	Length of Initial Term <i>(maintenance only)</i>	% 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



EPMO Project Proposal Request Form

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.



EPMO Project Proposal Request Form

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.



EPMO Project Proposal Request Form

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		\$	\$	\$			



WSIA Comments on the proposed Centralized Cybersecurity Event Notification Portal Project March 6, 2026

The Wholesale and Specialty Insurance Association (WSIA) would like to thank the Cybersecurity Working Group for the opportunity to review and comment on the revised project proposal for the NAIC Centralized Cybersecurity Event Notification Portal. We appreciate the idea of a licensee-directed cybersecurity event notification portal and we think a well-crafted portal could benefit our members.

After reviewing the recent revisions to the proposal, WSIA and our members respectfully submit the following questions to clarify our understanding of the proposed portal and its potential benefits and risks for our membership. We believe addressing these questions in the revised proposal—prior to its submission to the H Committee for broader member input and strategic alignment—will enable a more informed discussion.

Regulator Access

- **Improved Clarity:** Section 2 – Proposed Solution & Section 6 – Key Success Metrics
 - Both sections have undergone significant revisions to more closely align with a *“push-based, licensee directed system.”*
- **Concern remains:** Section 7 – Customer Segments
 - This section states *“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 are available.”*
 - This statement calls into question the proposed solution that regulator access will be limited to only those departments with state law adopting Model #668 and the responsibility for selecting those departments will be upon the licensee.
 - **Regarding regulator access to portal notifications, what does “legally entitled to” mean? Within the context of this proposal, this term is vague and could be broadly interpreted to shift the data access standard from licensee driven to regulator discretion.**

Cost

- **Concern remains:** Section 5 – Value Proposition, Section 8 – Cost Structure, Section 13 – Revenue Streams/Sources, & Section 14 – Recoup Costs
 - While the revised proposal suggests the portal will reduce licensee compliance costs, all references to portal cost estimates, an administrative fee model from licensees, and additional fees charged to recoup portal costs have been removed and replaced with a statement that new estimates will be made available and that revenue generation capability may be explored later.
 - **The revised proposal fails to explore the cost of developing and maintaining the portal. Should licensees anticipate fees associated with submitting portal notifications to fund the development and maintenance of the portal?**

Conclusion

WSIA would like to thank you for seeking interested party input, expertise, and feedback on the Centralized Cybersecurity Event Notification Portal project proposal. Again, we believe addressing these questions in the revised proposal—prior to its submission to the H Committee for broader member input and strategic alignment—will enable a more informed discussion. WSIA stands ready to work with the Cybersecurity (H) Working Group and the Cybersecurity, and Technology Committee (H) Committee to provide additional information, input, or feedback. Thank you for your consideration.

Sincerely,

A handwritten signature in black ink, appearing to read "John Meetz", with a stylized flourish at the end.

John H. Meetz
Director of Government Relations
Wholesale and Specialty Insurance Association (WSIA)
john@wsia.org
816.799.0863