Attachment 1

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~~event, adding significant costs to an already expensive process, and increases legal risk due to inconsistent compliance expectations. Additionally, this complexity is a friction point for the industry as legislatures consider the adoption of MDL #668, as licensees must bear additional compliance requirements. Lastly, the Cybersecurity (H) Working Group has charges that would be imperiled by inaction or failure, particularly charges #3 and #8. Without the additional efficiency a central portal would create, developing guidance for cyber events and coordinating any ~~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.

Commented [KH1]: Revised to reflect feedback received from Northwestern Mutual

The Cybersecurity (H) Working Group has been working to align the various areas of MDL #668 and the centralized cybersecurity event notification portal is the final piece. Already, guidance documents have been adopted to reduce the compliance burden of industry by aligning the efforts of departments of insurance as they enforce sections 6 and 7: the Cybersecurity Event Response Plan (CERP), and the Insurance Data Security Model Law Compliance and Enforcement Guide. While both have been adopted and address necessary areas of convergence, the ability to centralize the reporting of cybersecurity events requires technology, not a guide. This project is that technology.

The basic technology underlying the portal, being able to store and receive highly sensitive information while limiting access to only the appropriate users and aligning with well recognized control frameworks and will include clear governance over security, ~~is~~ 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 [KH2]: Revised to reflect edits received from Northwestern Mutual

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 (attachment 1). Data access will be highly limited to only those departments with an adopted version of MDL #668, and the responsibility for selecting those departments will be upon the licensee. ~~Lastly, s~~Additionally, security concerns should be assuaged by an annual disclosure of a System and Organization Controls Reporting (SOC) 3 report by the NAIC. The SOC 3 report is the public version of the NAIC's SOC 2 Type II that is conducted annually, and their report looks at the Security Trust Services Criteria.

Commented [MP3]: AHIP & Other Stakeholders: I'm including the current draft version of the standard form for clarity. Additional work is still required for regulators to validate that the standard form accurately reflects their laws.

Commented [MP4]: AHIP - Additional detail on the TSC that are tested: Security

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

Commented [MP5]: Michigan - A misunderstanding of how the phased approach should be handled caused this issue. This change is intended to fix the earlier oversight.

Key Features

- Licensee fills out a single, standard notification form, which may be updated as additional facts become known. A draft version of the standard form can be found in attachment 1, where additional details about uploading files can be found.
- Licensee directs notifications by selecting the departments to notify, which may be updated. Secure, role-based access for regulators, providing access only for those who have passed an equivalent to Section 6 of MDL #668.

Commented [MP6]: Michigan - A misunderstanding caused this fact to be overlooked from Michigan's comment letter. This change is intended to fix the earlier oversight.

- Regulators to have the ability to satisfy recordkeeping requirements by downloading completed records.

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

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

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

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

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

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

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

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

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

   The key deliverables necessary to make this project a success would include developing a portal that:

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

   To measure the success of the proposed centralized portal for cybersecurity event notifications, the following key metrics may be considered:

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

7. **CUSTOMER SEGMENTS:** **When answering this question, please describe:**
   - *What is the impact to the organization, members, another project or NIPR if this project is not approved?*
   - *Who is the customer/member? Who is your audience?*
   - *Who are the business owners/stakeholders that will be impacted by this?*

- *Who are the end users?*

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

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

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

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

Staffing Options & Estimate:

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

Assumptions:

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

The following phases are recommended:

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

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

Staffing Options/Estimates

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

Cost: $0 consulting costs – NAIC internal labor only

Duration: 7.5-8 months

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

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

Duration: 9.5-10 months

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

Cost: $2.1M consulting costs, and reduced capacity of NAIC staff working with outside firm

Duration: 7.5-8 months

~~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?*

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

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

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

Risk: Access and confidentiality protections for licensees.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Commented [MP7]: WSIA & NAMIC - answer to question on cost: No cost to licensees is anticipated in the future.

AHIP - while less detail than requested vis a vis a cost recovery model, this should provide adequate predictability to licensees at this point in development.

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

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

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

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

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

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

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

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

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

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

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

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

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

- It is assumed that the number of workforce identities will remain consistent at 1,000 over the 3-year term. While this number is currently accurate, the NAIC may experience growth.
- The estimates assume that the implementation and integration of the Identity and Access Management (IAM) tool with existing systems (Active Directory, Okta, eDirectory, Workday) will be completed within the planned timeline without significant delays.
- It is assumed that internal teams, including the IAM team and identity teams, will be available and have the necessary expertise to support the implementation and integration efforts.
- The estimates assume that the selected IAM tool will be compatible with the NAIC's existing identity systems and will not require significant additional customization or development.

- The cost estimates do not include a managed service offering for ongoing support. The NAIC may choose to purchase this offering in the future.

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

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

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

☐ **HIGH**
Please comment:

☐ **MEDIUM**
Please comment:

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

-
-
-
-

For EPMO use only – do not fill out.

Attachment 1

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