

Confidential Cybersecurity Event Repository & Portal

A Proposal that Addresses All Stakeholder
Requirements

Proposal: Two Motions for One Project

- Creating a Confidential Cybersecurity Event Repository & Portal (the project) for the US insurance sector involves gaining the confidence of both industry and regulators.
- This will be done by splitting the project into two, with two motions to be adopted:
 - The first motion would create a minimally functional portal at the NAIC so security and access controls reasonably related to confidentiality can be robustly tested for industry.
 - The second motion will seek to implement the portal into use for those states that have passed the Insurance Data Security Model Law #668, and to plot future improvements achieve regulatory convergence.

Background: Cybersecurity Event Response Plan (CERP) - Overview


The CERP, adopted during the 2024 NAIC Spring Meeting, provides departments of insurance guidance on the cybersecurity event notification process detailed in Section 6 of the Insurance Data Security Model Law #668 (MDL-668).

Guidance on the process emphasizes the primary role of the licensee to perform an investigation and the role of the department to collect the required information without unduly burdening the licensee.

Confidentiality of cybersecurity event information is required by Section 8 of MDL-668 and the CERP makes clear each department's responsibility in maintaining such confidentiality.

Background: The One-to-Many Reporting Problem

While the CERP will serve as a tool to assist with bringing convergence to the cybersecurity event reporting process, it does not alleviate the underlying burden of notifying dozens of jurisdictions, some with varying requirements.



Not only does this regulatory fragmentation add risk to licensees who must also handle a cybersecurity event, it hinders further adoption of MDL-668.



Solving the One-to-Many reporting problem will streamline the reporting process and eliminate the increasing regulatory burden that occurs each time MDL-668 is passed by another jurisdiction.

Background: Early Concept – Confidential Repository

- The ability to satisfy the commitments both in the CERP and Section 8 of MDL-668 with a confidential repository at the NAIC was explored.
- Confidentiality, from a technical standpoint, is achieved through security and access controls, both of which the NAIC has years of practical experience in implementing and enforcing.
- After the concept was presented to regulators in March 2024 discussions with NAIC staff from the CTO's office made clear that the confidentiality requirements were technically feasible.

Where We Are Today: A Motion to Build & Test

- Developer hours cannot be allocated to a project without a project plan that's adopted within a motion.
- A motion that upon adoption by the working group will tie the following together:
 - Build out a project plan that can produce a portal that performs how MDL-668 requires. The completed portal will be tested for industry to demonstrate its confidentiality capabilities.
 - Build out a testing plan that leverages the full range of capabilities as well as one that will be readily accepted as satisfactory by industry.
 - Survey those States who have passed a version of MDL-668 to understand any variation from MDL-668 so that each legislative version can be fully reflected in future improvements to the portal.

Step 1: Portal Project Plan

- Keeping the scope of the project as tight as possible will best ensure its success. We keep the project's scope narrow by:
 - Building a portal that is only available to those states who have passed a version of MDL-668.
 - The portal will only support the questions found in Section 6B of MDL-668.
 - All features will reflect the statutory construction of MDL-668.
- However, this is not a perfect solution:
 - Some states have other, unique questions than those found in Section 6B.
 - Despite the proliferation of notification requirements across many economic sectors, the portal's initial project plan will only support MDL-668.

Step 2: Portal Testing Plan

- Using synthetic data generated from AI will allow us to simulate different cybersecurity events, allowing industry and other stakeholders to understand how cybersecurity event/incident data will be accessed by regulators.
- We propose using tabletop exercises to demonstrate a system's ability to adhere to confidentiality rules to all stakeholders. The idea for a tabletop demonstration was the brainchild of Allison Parent of GMFA, an important industry group.
- This sort of venue and the ability for industry to gain insight into the implemented confidentiality regime will allow for a productive discussion on its adequacy.

Step 3: Survey & Converge MDL-668 States

- Concurrent with the testing plan, a survey to better understand what states are doing with their own MDL-668 implementations will be sent out.
- The survey will seek to not only understand how each has implemented their law, but also any specific differences between the model and what their legislature produced so that future improvements can be made, and regulatory convergence achieved.
- None of the potential changes will have any impact on the confidentiality regime implemented for the project.

An Outline of the First Motion

- Let's summarize what's being proposed for a potential first motion:
 - Construct a portal at the NAIC
 - Portal design will be minimal, reflecting only the functionality of Section 6 of MDL-668, with plans to improve it over time to reflect actual legislation.
 - The portal will be used to test the applicable security and access controls to demonstrate that industry data is kept confidential as required by MDL-668.
 - Concurrent with the testing a survey will be sent to states to understand what's required to bring the portal's design in synch with existing legislation.

An Outline of the Second Motion

- After the completion of work required within the adopted first motion, a second motion will be necessary.
- The second motion will focus on implementation and regulatory convergence.
- Immediate implementation of a minimal portal will greatly reduce regulatory burden and simplify the cybersecurity event notification process for all MDL-668 states.
- The survey to states who have passed MDL-668 and the plan to perform future improvements to achieve regulatory convergence will be a project plan for consideration.

Summary: Two Motions for One Project

The project plan of the First Motion should produce the following:

- A centralized portal that allows licensees to notify those commissioners of insurance whose legislatures have passed a version of MDL-668 simultaneously.
- This portal will have been run through robust testing for the benefit of industry, who will be reasonably satisfied with its confidentiality regime.
- We will have the results of a survey and a plan to fix the portal's limited capabilities for those states whose legislatures have deviated from MDL-668's model language.



The project plan of the Second Motion should produce the following:

- An implementation plan to bring the existing portal into service.
- A plan for future improvements to achieve regulatory convergence.



Questions?

All comments and thoughts are encouraged