Confidential Cybersecurity Event Repository & Portal

A Proposal that Addresses All Stakeholder Requirements

Proposal: Two Motions for One Project

- Creating a Confidential Cybersecurity Event Repository &

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: Early Concept – Confidential Repository

- The ability to satisfy the commitments both in the CERP and Section 8 of MD-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.

- Developer hours cannot be allocated to a project without a project plan's adopted within a motion.

-

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 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 MFDR states.

- The survey to states who have passed MFDR and the plan to perform future improvements to achieve regulatory convergence will be a project plan for consideration.

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

-

Questions?

All comments and thoughts are encouraged