Discuss the Cybersecurity Event Notification Portal Project Memorandum

Attachment C

Michael Peterson (VA)

Why a Centralized Cybersecurity Event Notification Portal?

- Fragmented reporting across states creates inefficiencies and delays
- Over 1,000 annual notifications reported by states using MDL #668
- Current methods: emails, web forms, state-specific portals: varying in security and auditability
- Stakeholder feedback highlights the need for harmonization and confidentiality

Project Vision and Objectives

- **Goal:** Streamline and secure the reporting of cybersecurity events to state insurance regulators.

- **Foundation:** Built on MDL #668 and the Cybersecurity Event Response Plan (CERP)

- **Key Features:**
  - Unified NAIC-hosted platform
  - Real-time alerts and audit trails
  - Licensee ability to update/amend notices
  - Confidentiality and data integrity by design

Development Roadmap

- Build portal aligned with MDL #668 Section 6B
- Conduct security and confidentiality testing
- Survey MDL #668 states to support convergence and gather implementation insights
- Stakeholder engagement through workshops, roundtables, and feedback loops

Benefits and Value Proposition

- Reduces regulatory fragmentation and reporting burden
- Enhances incident response and oversight
- Builds industry trust through secure, confidential handling
- Backed by early interest from 6+ states and industry groups

Notification Practices Research

- Preliminary findings suggest notification practices vary more than anticipated
- Need to research whether notification practices differing are a matter of practice or law
- This information has a direct impact on the functionality and development of the portal
- When complete, the resulting documentation revisions will be made to allow for a full public comment period