NAIC NATIONAL MEETING
SUMMER 2022

Date: 7/12/22

Virtual Meeting
(in lieu of meeting at the 2022 Summer National Meeting)

CYBERSECURITY (H) WORKING GROUP
Thursday, July 14, 2022
3:00 – 4:00 p.m. ET / 2:00 – 3:00 p.m. CT / 1:00 – 2:00 p.m. MT / 12:00 – 1:00 p.m. PT

ROLL CALL

Cynthia Amann, Co-Chair	Missouri	Van Dorsey	Maryland
Wendy Erdly, Co-Chair	New York	Jake Martin	Michigan
C.J. Metcalf, Co-Vice Chair	Illinois	Troy Smith	Montana
Michael Peterson, Co-Vice Chair	Virginia	Martin Swanson	Nebraska
Sian Ng-Ashcraft	Alaska	Barbara D. Richardson	Nevada
Evan G. Daniels	Arizona	David Bettencourt	New Hampshire
Mel Anderson	Arkansas	Keith Briggs	North Carolina
Damon Diederich	California	Colton Schulz/Chris Aufenthie	North Dakota
Wanchin Chou	Connecticut	Don Layson/Todd Oberholtzer	Ohio
Matt Kilgallen	Georgia	Dan Petterson	Vermont
Lance Hirano	Hawaii	John Haworth	Washington
Shane Mead	Kansas	Rachel Cissne Carabell	Wisconsin

NAIC Support Staff: Miguel Romero/Frosty Mohn

AGENDA

1. Discuss its Work Plan for 2022—*Wendy Erdly (NY)* — Attachment 1

2. Receive an Update on the Implementation of the *Insurance Data Security Model Law* (#668)—*Holly Weatherford (NAIC)* — Attachment 2

3. Receive an Update on Federal Activity Related to Cybersecurity —*Brooke Stringer (NAIC)*

4. Receive an Update on the NAIC's Cybersecurity Tabletop Exercises —*Frosty Mohn (NAIC)*

5. Receive an Update on State Insurance Regulator Cybersecurity Tools —*Miguel Romero (NAIC)* — Attachment 3

6. Discuss Any Other Matters Brought Before the Working Group —*Wendy Erdly (NY)*

7. Adjournment

The Cybersecurity (H) Working Group 2022 Workplan:

Working Group Charges:

A. Monitor cybersecurity trends such as vulnerabilities, risk management, governance practices and breaches with the potential to affect the insurance industry.
B. Interact with and support state insurance departments responding to insurance industry cybersecurity events.
C. Promote communication across state insurance departments regarding cybersecurity risks and events.
D. Oversee the development of a regulatory cybersecurity response guidance document to assist state insurance regulators in the investigation of insurance cyber events.
E. Coordinate NAIC committee cybersecurity work including cybersecurity guidance developed by the Market Conduct Examination Guidelines (D) Working Group and the Information Technology Examination (E) Working Group.
F. Advise on the development of cybersecurity training for state insurance regulators.
G. Work with the Center for Insurance Policy and Research (CIPR) to analyze publicly available cybersecurity related information.
H. Support the states with implementation efforts related to the adoption of *Insurance Data Security Model Law* (#668).
I. Engage with federal and international supervisors and agencies on efforts to manage and evaluate cybersecurity risk.

- Workstream 1: Survey

Subject Matter Expert Group Lead: Pending

Summary: The Working Group could develop a survey intended to understand existing state resources and needs on the topic of cybersecurity. A survey could help in prioritizing the Working Group's training efforts and identify the relevant tools/resources could be useful to the regulator community.

Related Charges: This project would fall under charges A and G.

Considerations: Regulators should consider:

- Whether support for a survey project exists
- At what level the survey should be drafted

- Workstream 2: Cybersecurity Response Plan

Subject Matter Expert Group Lead: Pending

Summary: Regulators could develop an optional guide to assist states in responding to cybersecurity events among their regulated entities. The project could include:

- Outreach to regulators to determine helpful topics to be covered
- A Review of existing regulator cybersecurity response plans
- Drafting a response plan

Related Charges: This project would fall under charges B, C, and D.

Considerations: Regulators should consider:

- Whether support for a response plan exists
- Whether the publication should be regulator only or public
- Whether the project should only be undertaken after the survey project is completed

---

- Workstream 3: Monitoring

Subject Matter Expert Group Lead: N/A

Summary: The Working Group has several charges that relate to monitoring and coordination. At rotating meetings, regulators could receive updates from NAIC staff or regulators:

- Cybersecurity trends
    - Industry may also assist in the identification of relevant trends
- The relevant work done at the Market Conduct Examination Guidelines (D) Working Group and the Information Technology Examination (E) Working Group
- State efforts to implement/adopt the *Insurance Data Security Model Law* (#668)
- The relevant work done at federal and/or international

Related Charges: This project would fall under charges A, C, and D.

Considerations: With each item discussed, it would be relevant to consider if the Working Group should take an action which would be tailored to the situation. It's most likely that federal/international work would lead to such action/responses.

- Workstream 4: Training

Subject Matter Expert Group Lead: N/A

Summary: The Working Group could work with NAIC staff, regulators, and industry to identify cybersecurity subject matter that warrant training. The Working Group could then oversee the development of training.

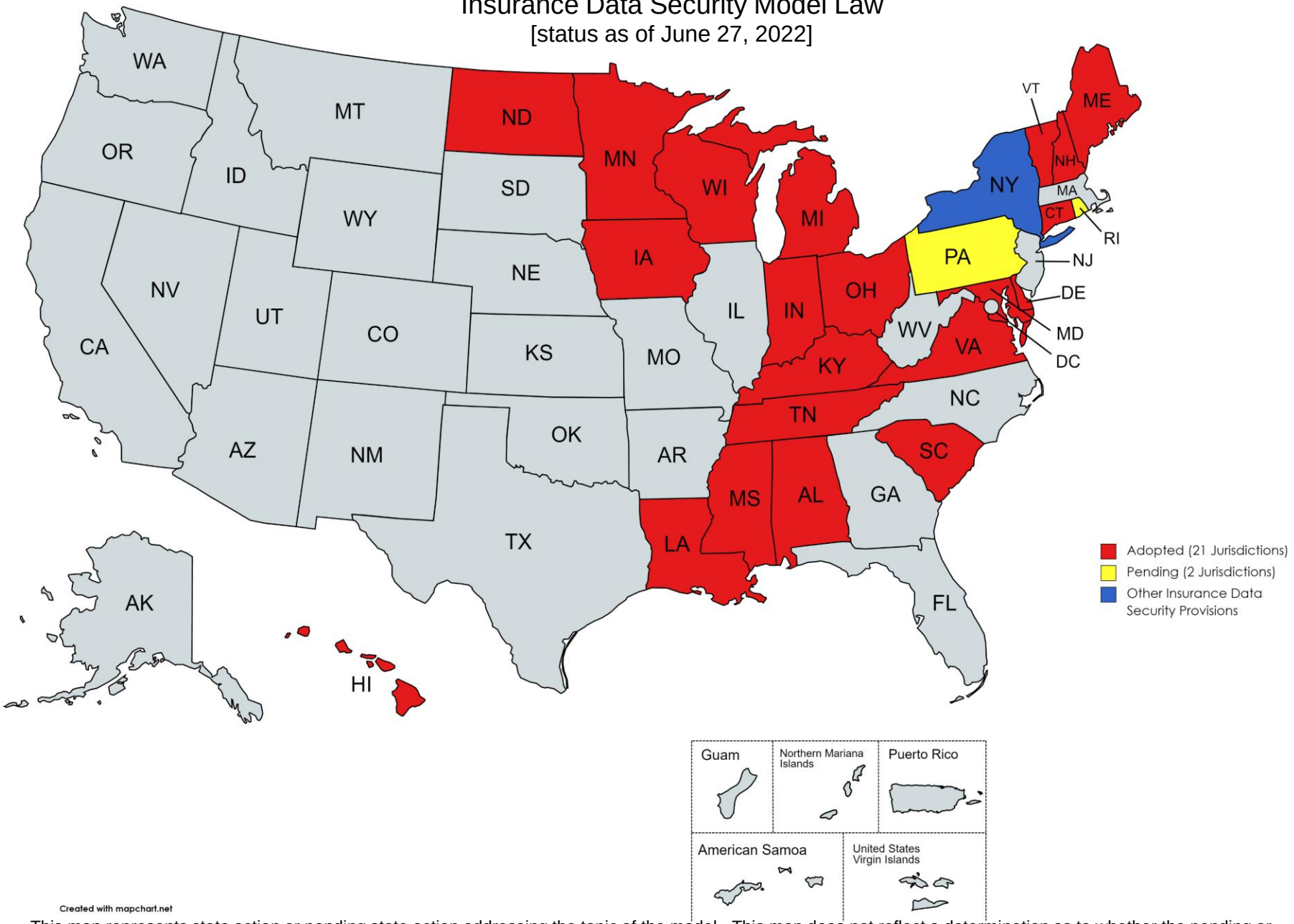
The Working Group could also work with D/E committee groups to help identify relevant certifications/credentials that Departments of Insurance could use to help in developing subject matter expertise.

Related Charges: This project would falls primarily under charge F but the subject matter that is trained on could relate to any of the other charges.

Considerations: While there are many topics that could warrant training, resource limitations will make it important to prioritize training requests in light of the significance/prevalence/complexity of said subject matter.

Attachment 2

Implementation of Model Act #668
Insurance Data Security Model Law
[status as of June 27, 2022]



This map represents state action or pending state action addressing the topic of the model. This map does not reflect a determination as to whether the pending or enacted legislation contains all elements of the model or whether a state meets any applicable accreditation standards.

NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

MEMORANDUM

TO: Members of the Cybersecurity (H) Working Group

FROM: NAIC Staff

DATE: May 2, 2022

RE: Summary of Cybersecurity Tools

With the creation of the Cybersecurity (H) Working Group and the addition of new voices to our discussion, NAIC staff have created this primer describing currently available NAIC cybersecurity-related regulatory tools.

There are three key NAIC resources regulators that relate to insurer cybersecurity – the NAIC's *Insurance Data Security Model Law* (Model #668), the *Financial Condition Examiners Handbook*, and the *Market Regulation Handbook*. This memo will summarize how each tool addresses the topic of cybersecurity as well as the interrelationship between each tool.

Insurance Data Security Model Law (#668)

The Model Law was adopted in 2017 and it builds on the existing broad regulatory authority vested in state insurance regulators. Specifically, it establishes standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event. Among the sections of the Model Law are:

- Information Security Program – This section sets expectations for what shall be included within a security program for licensees, with a specific discussion of mitigation practices that should be considered. The section also sets forth expectations for board oversight and oversight of third-party service providers.
- Notification of Cybersecurity Event – This section sets a 72-hour notification notice to the Commissioner for security events.
- Power of the Commissioner – This section gives the Commissioner the power to investigate licensees to determine if the licensees have engaged in any conduct in violation of the law.

Financial Condition Examiners Handbook

Financial exams serve a broad purpose but generally give regulators a chance to review and evaluate the financial condition and prospective solvency of insurers.

As part of the exam process, regulators perform a General Information Technology Review which has historically been focused on evaluating IT general controls and application controls. However, given the rise of cybersecurity concerns and the potentially for overlapping concepts/questions, the IT review also allows regulators to evaluate cybersecurity specific risks and controls.

The *Financial Condition Examiners Handbook* includes guidance based on the COBIT 5 Framework that provides regulators with possible questions aiding in the process of investigation. However, starting with

the 2016 edition of the *Financial Condition Examiners Handbook* and in subsequent editions, the guidance has been revised based on industry trends, to align with the Model Law, and to benefit from NIST Cybersecurity Framework concepts.

IT review guidance in the *Financial Condition Examiners Handbook* is maintained by the Information Technology (IT) Examination (E) Working Group. Moreover, the Working Group has an ongoing mandate to monitor cybersecurity trends and develop updates to guidance as needed.

Working with NAIC staff, the Working Group also developed a mapping tool that allows regulators to see how examination procedures relate to the Model Law and the guidance in the *Market Regulation Handbook* with the intent of creating efficiencies where possible.

Market Regulation Handbook

Following the adoption of the NAIC's Model Law, Market Conduct regulators added guidance in the *Market Regulation Handbook* to aid jurisdictions in reviewing a regulated entity's insurance data security program and response to a Cybersecurity Event.

The Market Conduct guidance comes in the form of two checklists. A "Insurance Data Security Post-Breach Checklist" was developed to allow market regulators to review a regulated entity's insurance data security program and response to a Cybersecurity Event, for compliance with applicable state statutes, rules or regulations relating to Model #668. The "Insurance Data Security Pre-Breach Checklist" was also developed; it is used by market regulators proactively, to understand regulated entity compliance with applicable state statutes, rules or regulations relating to Model #668, in the absence of a Cybersecurity Event.

The Insurance Data Security Pre-and Post-Breach Checklists are in the *Market Regulation Handbook* and are maintained by the Market Conduct Examination Guidelines (D) Working Group.

Cybersecurity Vulnerability Response Plan

To aid states in addressing matters related to vulnerabilities, the Information Technology Examination (E) Working Group developed a *Cybersecurity Vulnerability Response Plan*

The document guides examiners and/or analysts through the ad-hoc inquiry that may be necessary when a cybersecurity exposure or vulnerability has been identified or alleged in the period between full-scope examinations. It is, however, up to those examiners or analysts to use sound professional judgement when deciding to undertake such inquiries.

The results of the ad-hoc inquiry may warrant additional investigation, which could include calling a targeted examination, performing interim work, and/or follow-up on recommendations by the department analyst. If additional investigation is warranted, the vulnerability plan directs regulators consult the *Financial Condition Examiners Handbook* to identify relevant follow up procedures.

If there are any questions or concerns, please contact Miguel Romero at maromero@naic.org.