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* (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. If, during such inquiry, regulators identify the occurrence of a cybersecurity event, the Response Plan then directs regulators to use the post-breach checklist from the *Market Regulation Handbook.* 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.