The NAIC Insurance Data Security Model Law

- *Protecting consumer information is a high priority for insurance regulators in the wake of several major insurer data breaches.*
- *The NAIC Insurance Data Security Model Law (#668) seeks to establish data security standards for regulators and insurers in order to mitigate the potential damage of a data breach. The law applies to insurers, insurance agents and other entities licensed by the state department of insurance.*
- *The U.S. Treasury Department has urged prompt action by states to adopt the NAIC Insurance Data Security Model Law within the next 5 years or the administration will ask Congress to preempt the states.*

Background

In recent years, there have been several major data breaches involving large insurers that have exposed and compromised the sensitive personal information of millions of insurance consumers. As a result, state insurance regulators made reevaluation of the regulations around cybersecurity and consumer data protection a top priority, and in early 2016 the NAIC began drafting the Insurance Data Security Model Law. The model was adopted by the NAIC in October 2017 following almost two years of extensive deliberations and input from state insurance regulators, consumer representatives, and the insurance industry. State adoption of the model is critical for state insurance regulators to have the tools they need to better protect sensitive consumer information.

The model requires insurers and other entities licensed by a state department of insurance to develop, implement, and maintain an information security program based on its risk assessment, with a designated employee in charge of the information security program (Section 4). The model phases in requirements for compliance with the information security program and oversight of third-party service providers. Licensees determine the appropriate security measures to implement based on careful, ongoing risk assessment for internal and external threats. The model also requires licensees to investigate a cybersecurity event (Section 5) and notify the state insurance commissioner of a cybersecurity event (Section 6). It also grants insurance commissioners the power to examine and investigate licensees to determine compliance with the law, and provides state insurance regulators the authority to remedy data security deficiencies they find during an examination. The model exempts licensees with fewer than 10 employees, licensees compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and agents of a licensee from Section 4 of the model. The model does not create a private cause of action, nor does it limit an already- existing private right of action.

In an October 2017 report on the asset management and insurance industries, the U.S. Treasury Department recommended prompt adoption of the model by the states. Treasury further recommended that if adoption and implementation of the model by the states does not result in uniform data security regulations within five years, then Congress needs to act by passing legislation setting forth uniform requirements for insurer data security.

Key Points

- To date, the NAIC *Insurance Data Security Model Law* (#668) has been adopted in 13 states: AL, CT, DE, IN, LA, ME, MI, MS, ND, NH, OH, SC and VA.
- The NAIC Insurance Data Security Model law was developed in response to high-profile data breaches of insurers and other institutions.
- The model requires insurers and other entities licensed by the department of insurance to develop, implement and maintain an information security program, investigate any cybersecurity events and notify the state insurance commissioner of such events.
- The federal government has urged states to adopt the model law.

Holly Weatherford, Senior Legislative Affairs Counsel, hweatherford@naic.org
Jennifer McAdam, Senior Counsel, jmcadam@naic.org
Chara Bradstreet, Chief of State Relations & Policy Advisor, cbradstreet@naic.org