**PROJECT HISTORY - 2017**

**INSURANCE DATA SECURITY MODEL LAW (#668)**

**1. Description of the Project, Issues Addressed, etc.**

The Cybersecurity (EX) Working Group, previously known as the Cybersecurity (EX) Task Force, was established by the NAIC's Executive (EX) Committee in 2014 to consider issues concerning cybersecurity as they pertain to the role of state insurance regulators. In 2015, the Working Group created two documents that were adopted by the NAIC: 1) *Principles for Effective Cybersecurity: Insurance Regulatory Guidance*, adopted in April 2015; and 2) *NAIC Roadmap for Cybersecurity Consumer Protections*, adopted in December 2015. Also, in 2015, Congress introduced a bill, the Data Security Act of 2015 (H.R. 2205). The NAIC and interested parties had concerns about this legislation and determined that the best way to proceed was with a model law specific to the insurance industry. Before determining that one new model was the appropriate course of action, the Working Group considered amending four different model laws related to data privacy: 1) the *NAIC Insurance Information and Privacy Protection Model Act* (#670); 2) the *Privacy of Consumer Financial and Health Information Regulation* (#672); 3) the *Standards for Safeguarding Consumer Information Model Regulation* (#673); and 4) the *Insurance Fraud Prevention Model Act* (#680).

The Working Group began drafting the Insurance Data Security Model Law in early 2016. The major provisions of the model include requiring insurers and other entities licensed by the department of insurance to: implement an information security program (Section 4); investigate a cybersecurity event (Section 5); and notify the state insurance commissioner of a cybersecurity event (Section 6).

The Working Group adopted the Insurance Data Security Model Law on Aug. 7 at the 2017 Summer National Meeting and presented it to the Innovation and Technology (EX) Task Force. The Task Force adopted the Insurance Data Security Law on Aug. 8 at the 2017 Summer National Meeting.

**2. Name of Group Responsible for Drafting Model and States Participating**

The Cybersecurity (EX) Working Group, previously known as the Cybersecurity (EX) Task Force, drafted the model law. The members of that Task Force at the time of adoption were: South Carolina, Chair; Rhode Island, Vice Chair; Alaska; Arkansas; California; Colorado; Connecticut; Delaware; District of Columbia; Florida; Idaho; Illinois; Kansas; Kentucky; Maine; Maryland; Michigan; Minnesota; Missouri; Montana; Nebraska; Nevada; New Hampshire; New Jersey; New Mexico; North Dakota; Northern Mariana Islands; Ohio; Oklahoma; Oregon; Pennsylvania; South Dakota; Tennessee; Texas; Utah; Vermont; Virginia; Washington; and Wisconsin.

In November 2016, the Working Group formed a drafting group, consisting of industry, consumer representatives and state insurance regulators. This group included representatives from the following interested parties: American Council of Life Insurers (ACLI), America's Health Insurance Plans (AHIP), the American Insurance Association (AIA), the American Land Title Association (ALTA), the Independent Insurance Agents and Brokers of America (IIABA), the National Association of Mutual Insurance Companies (NAMIC), the Professional Insurance Agents (PIA), the Property Casualty Insurers Association of America (PCI), the Reinsurance Association of America (RAA), the Center for Economic Justice (CEJ) and Peter Kochenburger (University of Connecticut School of Law). The drafting group also included state insurance regulators from California, Florida, Illinois, Maine, New York, Rhode Island and Texas.

**3. Project Authorized by What Charge and Date Given to the Group**

The original charge of the Cybersecurity (EX) Working Group, previously known as the Cybersecurity (EX) Task Force, was to: review the following models and make recommendations to the Executive (EX) Committee: the *NAIC Insurance Information and Privacy Protection Model Act* (#670); the *Privacy of Consumer Financial and Health Information Regulation* (#672); the *Standards for Safeguarding Consumer Information Model Regulation* (#673); and the *Insurance Fraud Prevention Model Act* (#680).

During the Working Group's meeting at the 2016 Spring National Meeting, on April 4, the Working Group determined that it would be simpler to draft one new model law and address any revisions to the other models at a later date, if necessary.

 

**4. A General Description of Drafting Process and Due Process**

The Cybersecurity (EX) Working Group, previously known as the Cybersecurity (EX) Task Force, released the first draft of the Insurance Data Security Model Law on March 2, 2016. Following a 30-day exposure period, interested stakeholders presented comments during the Working Group's April 4, 2016, conference call.

The Working Group held an interim meeting May 24–25, 2016, and received section-by-section oral comments regarding the first draft of the model law.

The Working Group met via conference call Aug. 4, Aug. 11 and Aug. 16, 2016, in regulator-to-regulator session pursuant to paragraph 3 (specific companies, entities or individuals) and paragraph 8 (consideration of strategic planning issues) of the NAIC Policy Statement on Open Meetings. The second draft of the model law was released on Aug. 17, 2016. Oral comments regarding the second draft were received on Aug. 27 via conference call, and written comments were received by Sept. 16, 2016, following a 30-day exposure period.

The Working Group met via conference call Oct. 17, 2016, to discuss the second draft of the model law, as well as to receive additional oral comments. Subsequently, the Working Group met via conference call Nov. 8, 2016. During this meeting, the Working Group formed a drafting group to continue drafting the model law. The drafting group included state insurance regulators and interested parties. Between versions two and three of the model, the drafting group met via conference call on following dates in 2016: Nov. 15, Nov. 22, Nov. 29 and Dec. 20. It also met on the following dates in 2017: Jan. 10, Jan. 24, Feb. 7 and Feb. 21.

The drafting group released a third version of the draft model law on Feb. 27, 2017. The drafting group met via conference call March 7 to continue discussion regarding the third draft of the model law. Written comments were received from interested stakeholders through April 17.

The drafting group released a fourth draft of the model law on April 26. The drafting group met via conference call May 9 to discuss the fourth version of the model. Oral comments were received on the May 9 conference call, and written comments were received from stakeholders by May 16, following a 20-day exposure period.

The drafting group released the fifth draft of the model law July 7. Written comments were received from interested stakeholders by July 31 following a 24-day exposure period. The Working Group adopted the fifth version of the model law with some minor changes at the Summer National Meeting. Due to the changes made, the Working Group adopted it as the sixth version of the model law.

The final version of the draft model law, the sixth draft, was adopted by the Innovation and Technology (EX) Task Force at the Summer National Meeting. Prior to consideration of adoption by the Executive (EX) Committee and the joint Executive (EX) Committee and Plenary, two technical corrections will be noted for incorporation into the final version of the model: 1) removal of a cross-reference to a provision that had been deleted from version five; and 2) clarification regarding implementation of security measures at Section 4D(2).

All drafts and comments were posted on the Working Group's web page on the NAIC website.

**6. A Discussion of the Significant Issues (items of some controversy raised during the due process and the group's response)**

The first version of the model was drafted by incorporating key provisions of the legislation pending in Congress, H.R. 2205 and a draft model law submitted by a group of several insurance trade associations. Key provisions of the first version included requiring a licensee to: 1) implement an information security program; 2) investigate a potential data breach; 3) notify consumers of their rights before a data breach; and 4) notify consumers following a data breach. It also provided the state insurance commissioner with authority to prescribe the appropriate level of consumer protection following a data breach.

Following a two-day in-person meeting with interested parties, the second version of the model law was released. Comments received following the exposure of the second version made it apparent there were six important issues on which the Working Group would need to reach consensus: 1) how to address state uniformity and exclusivity of the law; 2) whether and how to include an exemption for licensees subject to the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the federal Gramm-Leach-Bliley Act (GLBA); 3) whether to include a harm trigger in the definition of "data breach"; 4) how to define "personal information"; 5) how to address scalability of information security requirements for

smaller licensees; and 6) how to address licensee oversight of third-party service providers.

Considering the complexity of these issues, the Working Group created a drafting group to hold a number of in-depth discussions in an attempt to reach consensus. Following drafting group calls held between November 2016 and February 2017, a third version of the model was exposed. Comments received on the third version revealed that drafting group members still disagreed on how to address several of the key issues.

At the 2017 Spring National Meeting, Superintendent Maria T. Vullo (NY) urged the Working Group to adopt New York's *Cybersecurity Requirements for Financial Services Companies*, N.Y. Comp. Codes R. & Regs. tit. 23, § 500, as the NAIC's model law. At the Working Group's meeting on April 9 at the 2017 Spring National Meeting, drafting group chair Superintendent Elizabeth Kelleher Dwyer (RI) invited all interested parties to submit additional comments on the third version of the draft, as well as thoughts regarding Superintendent Vullo's proposal to redraft the model law to look more like the New York regulation.

After receiving letters from interested parties, a fourth draft was released that incorporated many of the provisions found in the New York regulation. Like the New York regulation, the fourth version of the model law delegates consumer notification of a cybersecurity event (data breach) to be done in compliance with the state's already-existing generally applicable data breach notification law, rather than create insurance-specific rules regarding consumer notification. Some of the provisions in version four of the model that were similar to the New York regulation included: 1) the same definition of "non-public information" that must be protected; 2) a similar definition of "cybersecurity event"; 3) risk management standards based on the licensee's own risk assessment; 4) similar language regarding oversight of third-party service provider arrangements; and 5) requirement of an incident response plan. The NAIC model also added exceptions to the law, which were similar to those found in the New York regulation, including: 1) licensees with fewer than 10 employees; and 2) licensees using the information security program of another licensee. The NAIC model also added an exemption for licensees compliant with HIPAA data security laws, which is not found in the New York regulation.

After receiving comments on version four of the model, several provisions were redrafted, including the addition of a drafting note to Section 2, stating that the intent of the drafters is that if a licensee is in compliance with the New York regulation, it is also in compliance with this model law. In response to industry comments that the provision addressing oversight of third-party service providers was burdensome, the provision was revised to require licensees to exercise due diligence in selecting its third-party service providers and to require those provides to implement appropriate measures to protect consumer data. The requirement of an annual report was revised to become a requirement of annual certification, which more closely mirrors language from the New York regulation.

The drafting group determined that certain issues raised by interested parties did not warrant changes to the model. Several interested parties requested reinstatement of language stating the model law is an "exclusive state standard." The original concern was related to inconsistencies regarding consumer notices, reflecting that approximately 48 states have specific and often differing laws on consumer notices applicable across industries. Since the model no longer requires consumer notice, apart from that already required by state law, the need for a statement of exclusivity was no longer present. Additionally, some interested parties suggested there was a need for stronger confidentiality protections, similar to those found in the *Risk Management and Own Risk and Solvency Assessment Model Act* (#505). But the heightened confidentiality protections of the Model #505 were drafted to protect information that includes trade secret and proprietary information, which is not the type of information provided to the state insurance commissioner under this model. The Working Group noted that the same confidentiality language that appears in this model law has been included in multiple NAIC models.

**7. Any Other Important Information (e.g., amending an accreditation standard)**

No other items are identified at this time.