ROLL CALL

Raymond G. Farmer, Chair
Elizabeth Kelleher Dwyer, Vice Chair
Lori K. Wing-Heier
Allen W. Kerr
Dave Jones
Marguerite Salazar
Katharine L. Wade
Trinidad Navarro
Stephen C. Taylor
David Altmaier
Dean L. Cameron
Jennifer Hammer
Ken Selzer
Brian Maynard
Eric A. Cioppa
Al Redmer, Jr.
Patrick M. McPharlin
Mike Rothman
Chlora Lindley-Myers
Matthew Rosendale
South Carolina
Rhode Island
Alaska
Arkansas
California
Colorado
Connecticut
Delaware
District of Columbia
Florida
Idaho
Illinois
Kansas
Kentucky
Maine
Maryland
Michigan
Minnesota
Missouri
Montana
Bruce R. Ramge
Barbara D. Richardson
Roger A. Sevigny
Richard J. Badolato
John G. Franchini
Jon Godfread
Mark O. Rabauliman
Mary Taylor
John D. Doak
Laura Cali Robison
Teresa D. Miller
Larry Deiter
Julie Mix McPeak
TBD
Todd E. Kiser
Michael S. Pieciak
Jacqueline K. Cunningham
Mike Kreidler
Ted Nickel
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
Wisconsin

AGENDA

1. Consider Adoption of its Spring National Meeting Minutes
   —Director Raymond G. Farmer (SC)  
   Attachment A

2. Hear an Update Regarding Federal Cybersecurity Legislation—Brooke Stringer (NAIC)

3. Hear a Report Regarding the Data Collected from the Cybersecurity Insurance Coverage Supplement of the NAIC 2016 Property/Casualty Annual Financial Statement and Surplus Lines Data Collection—Eric Nordman (NAIC)  
   Attachment B

4. Discuss the Insurance Data Security Model Law—Director Raymond G. Farmer (SC)

5. Consider Adoption of the Insurance Data Security Model Law—Director Raymond G. Farmer (SC)  
   Attachment C

6. Discuss Any Other Matters Brought Before the Working Group—Director Raymond G. Farmer (SC)

7. Adjournment

© 2017 National Association of Insurance Commissioners
2017 Summer National Meeting

Cybersecurity (EX) Working Group

August 7, 2017
Philadelphia, Pennsylvania
Attachment A

Consider Adoption of its Fall National Meeting Minutes
Date: 4/19/17

Cybersecurity (EX) Working Group  
(f.k.a., the Cybersecurity (EX) Task Force)  
Denver, Colorado  
April 9, 2017

The Cybersecurity (EX) Working Group of the Innovation and Technology (EX) Task Force met in Denver, CO, April 9, 2017. The following Working Group members participated: Raymond G. Farmer, Chair (SC); Elizabeth Kelleher Dwyer, Vice Chair (RI); Chris Murray (AK); Mel Anderson (AR); Susan Bernard and Bryant Henley (CA); Peg Brown (CO); Katharine L. Wade (CT); Sean O'Donnell (DC); Frank Pyle (DE); Susanne Murphy (FL); Tom Donovan (ID); Michael Rohan (IL); Ken Selzer (KS); Paula Keen (MD); Eric A. Cioppa (ME); Donna M. Watz (MN); Angela Nelson (MO); Mark O. Rabauliman (MP); Jon Godfread (ND); Martin Swanson (NE); Peter L. Hartt and Kristine Maurer (NJ); Barbara D. Richardson (NV); Jillian E. Froment (OH); Cuc Nguyen (OK); Laura Cali Robison (OR); Christopher Monahan (PA); Lorrie Brouse (TN); Rebecca Nichols (VA); Sandra Bigglestone, David Provost and Christina Rouleau (VT); Patrick McNaughton (WA). Also participating were: Jim L. Ridling (AL); Ralph T. Hudgens (GA); Artemio B. Ilagan (GU); Gordon I. Ito (HI); Doug Ommen (IA); Warren Byrd (LA); Maria T. Vullo (NY);

1. **Adopted its 2016 Fall National Meeting Minutes**

Superintendent Dwyer made a motion, seconded by Ms. Brouse, to adopt its Dec. 11, 2016, minutes *(see NAIC Proceedings – Fall 2016, Cybersecurity (EX) Task Force).* The motion passed unanimously.

2. **Heard an Update Regarding Federal Updates for Cybersecurity**

Brooke Stringer (National Association of Insurance Commissioners—NAIC) said the NAIC continues to engage with federal and state regulators through the U.S. Department of the Treasury’s (Treasury Department) Financial Banking and Information Infrastructure Committee (FBIIC), which facilitates coordination and communication on enhancing the cyber resiliency of the financial sector.

Director Farmer serves as the NAIC’s FBIIC representative and recently participated in the first meeting of the year with the new administration. Treasury Secretary Steven Mnuchin is focused on cybersecurity in the context of financial stability and has emphasized the importance of incorporating cybersecurity in financial oversight responsibilities.

The federal banking regulators released an advanced notice of proposed rulemaking on Enhanced Cyber Risk Management Standards last October. The proposal is a standards-based, tiered approach to establishing a cybersecurity framework with prescriptive standards. These standards would apply to insurance savings and loan holding companies and insurers that have been designated as systemically important financial institutions (SIFIs). The NAIC submitted a comment letter in February underscoring the importance of coordinating with state insurance regulators to strive for consistency to align cybersecurity regulatory guidance where possible, particularly for the insurance groups in which there is shared regulatory oversight. Currently, there is no indication of the timing of next steps for the rulemaking.

The National Institute of Standards and Technology (NIST) has issued a draft update to its Cybersecurity Framework. The framework is used by a broad array of businesses and organizations. The updated framework aims to further develop NIST’s voluntary guidance on reducing cyber risks, and the NIST anticipates publishing a final version this fall.

3. **Heard a Presentation from the NYDFS Regarding the Implementation and Status of its Cybersecurity Requirements for Financial Services Companies**

Superintendent Vullo said the institutions she regulates vary in size and risk. In February, New York issued its final cybersecurity regulation. New York’s cybersecurity regulation acknowledges that in the ever-increasing global and interconnected world, all financial institutions are vulnerable to cyberattack. Financial systems are under the constant risk of cybersecurity threats, including foreign and domestic, as well as internal and external. Superintendent Vullo said it is critical for financial institutions to be proactive and constantly evolving in order to stay ahead of cybersecurity threats.
The New York State Department of Financial Services (NYDFS) went through a thorough and fulsome process before issuing its cybersecurity regulation. The NYDFS studied the issue of cybersecurity two years prior to introducing the regulation, as well as engaged with stakeholders. The NYDFS exposed the initial regulation for comment in September 2016. Numerous meetings were held with insurers and others, in addition to receiving and reviewing written comments. Changes were made to the initial regulation to reflect the comments received. The regulation was released for a second comment period. The final regulation went into effect March 1, 2017. The regulation contains time frames regarding the implementation of the various provisions.

Superintendent Vullo said the comment period was an important part of the process. The NYDFS met with each of the constituencies involved in the regulation, including life insurers, health insurers, property insurers, brokers, agents and the third parties servicing these entities. The NYDFS also spoke with chief information security officers (CISOs), cybersecurity experts, law enforcement experts and New York’s cybersecurity board, on which Superintended Vullo serves as a member.

Superintendent Vullo said the NYDFS took great strides to ensure its regulation would create an achievable structure for institutions to tackle cybersecurity operationally and effectively. It is important for a regulation to be workable in practice. Entities are different, and there is no one-size-fits-all solution. The NYDFS spent a considerable amount of time differentiating between what should be a minimum standard and what should be a requirement. It was made clear that each individual institution’s solution is risk-based; each institution will assess its own risk and match its controls to those risks.

Superintendent Vullo said the regulation focuses on a framework, as well as minimum requirements. She said the NYDFS wanted to make sure its institutions have a critical infrastructure and governance on a scale appropriate to the individual institutions’ size and risk profile. The first principle of New York’s regulation requires an institution have a comprehensive cybersecurity policy and a cybersecurity program. The cornerstone of New York’s cybersecurity regulation is a risk assessment that each regulated entity must conduct by reviewing its own risks and controls to enable the design of appropriate measures to ensure the cybersecurity program works.

The NYDFS regulation requires entities to ensure they have adequate staff to address cybersecurity concerns, including a CISO. The CISO is required to periodically report to the board of directors of an organization regarding the cybersecurity program; this is a key element of the regulation. The regulation also includes training, monitoring and testing, and data retention. Regarding technical requirements, the regulation requires entities to design appropriate risk-based controls for access, including the utilization of multi-factor authentication to protect the most sensitive data. The regulation requires entities to use encryption or reasonable alternative compensating controls to protect personal data.

The New York regulation requires an entity to design appropriate controls to insure third-party vendors that access the data have appropriate controls in place. The impact of outsourcing of personal data regarding cybersecurity compliance cannot be ignored. The regulation requires the regulated entity to insure its vendors that have personal data have adequate cybersecurity protection.

The New York regulation requires minimum standards, while encouraging its institutions to keep pace with technological advances. The regulation includes risk-based language, where appropriate, to encourage the regulated entities to design risk-based solutions appropriate to the entity based on the type of information the institution receives and the systems the intuition has to protect their data. The regulation requires the cybersecurity program be adequately funded and staffed, overseen by qualified management; however, the regulation allows the entity to determine how it will fulfill the requirement based upon the entities risk assessment.

While the regulation requires robust access controls, which is the core of any cybersecurity program, the regulation leaves it to the entity to design the appropriate risk-based controls. The regulation also requires minimum standards to aid in addressing any cybersecurity breaches, including an incident response plan, preservation of data to respond to the breach and notice to the regulator of material events within 72 hours of the entity’s determination of a material breach. The regulation promotes accountability by requiring identification and documentation of material deficiencies, remediation plans and annual certifications of regulatory compliance. The regulation requires document retention, including an audit trail designed to protect and respond to cybersecurity events and systems sufficient to reconstruct material transactions. Superintendent Vullo said, as regulators, the NYDFS wants to create a culture of compliance where senior management takes the issue of cybersecurity seriously. The annual certificate of regulatory compliance requires certification that the cybersecurity program complies with its regulation. The process requires the board of directors, or senior management, to review the program on an
annual basis and take the steps to ensure the program is sufficient. The certification can be based on the best knowledge of the management, as well as the documents, reports and opinions of the employees with the day-to-day responsibility, or appropriate outside vendors that support the entity, following which the senior management must certify compliance to the regulator.

Throughout the drafting and redrafting of the regulation, the NYDFS took great care to create the appropriate standards. Superintendent Vullo said regulators seek consistency whenever possible. She said the NYDFS believes the best way for industry to focus on cybersecurity threat is to have a consistent framework. Superintendent Vullo said the NYDFS worked hard to get regulation right with extensive input from all stakeholders. She urged the Working Group and the NAIC to consider adopting the New York regulation as the model law.

Superintendent Vullo said the NYDFS does not believe incorporating the federal Gramm-Leach-Bliley Act (GLBA) as the baseline creates the additional standards needed. She stressed the NYDFS regulation does not conflict with GLBA or any other federal law. The NYDFS regulation builds on the core of non-specific flexible principles created by the GLBA with specific risk-based minimum requirements applicable to a regulator.

Superintendent Vullo said the NYDFS regulation also balances some of the concerns the Working Group has heard regarding the NAIC draft Insurance Data Security Model Law. Regarding incident reporting and breach notification, the NYDFS received many comments regarding the burden of regulation. New York’s regulation balances these concerns by requiring notices of significant cybersecurity events within 72 hours of a determination the event is material and reportable, not from discovery. The current draft of the NAIC model requires notice of data breaches within three days of determining a breach may have occurred. The NYDFS believes the word “may” is too vague to be workable in practice, leading to confusion over what is required to be submitted.

Superintendent Vullo said the NAIC draft model encourages entities to protect personal information by encryption or other appropriate means for data transmitted wirelessly or on a public network and all non-public personal information stored on a laptop or other portable device. The New York regulation’s encryption requirements are more specific, while continuing to be risk-based. The New York regulation requires a risk-based determination as to what should be encrypted and requires an entity’s CISO to review and approve any alternative compensating controls, to ensure they are effective should an entity chooses not to use encryption.

Director Farmer said one of the issues the Working Group has encountered is the notification to consumers. He asked Superintendent Vullo if the NYDFS addressed this issue. Superintendent Vullo said the New York regulation does not require the notification of consumers; however, there are requirements in the New York regulation that the institution, as part of its cybersecurity program, have an incident response plan and have the appropriate reporting. She said if an entity learns there is a data breach and personal data has potentially been affected, the entity’s incident response plan should include the notification of consumers as appropriate.

Mr. Henley said California is supportive of efforts regarding allowing individual states to adopt standards that are greater than the GLBA. He asked if Section 500.17 of the New York regulation deals with notices to the superintendent and requires that covered entities must notify the superintendent under: a) 1) a notice is required to be provided to any government body self-regulatory agency or any other supervisory body. He said he reads this to mean that if New York has a law requiring an entity to provide notice to said consumer, that law in turn would require notice to the superintendent. Superintendent Vullo said this is correct; however, she said it is much broader. She said there might be notices required under laws to other regulatory bodies, and the NYDFS wants to be sure that if there is notice to another regulatory body, that the NYDFS gets the notice at the same time. Superintendent Vullo said regulatory bodies could be both federal and state, and since the NYDFS also regulates the banking institutions, there would be many notices there as well. She said the NYDFS wanted to capture material events as they are defined in its regulation. Mr. Henley said this sounds like an elegant solution to a challenging problem.

Mr. Henley said are insurers, brokers and third-party service providers of various sizes and scope. He said New York’s regulations do not reference NIST standards or other standards in existence. Mr. Henley said California was informed the requirements given by the Center for Internet Security (CIS) reflected the minimum requirements that must be met. He said the advantage to using these standards are that these are clear standards that can be enforced against entities that fail to meet the standards. Mr. Henley asked if New York considered NIST standards and why it chose not to specifically incorporate
them by reference. Superintendent Vullo said NIST is updated on an ongoing basis and is a voluntary and best practices framework. She said the NYDFS thought it needed to set minimum standards, as well as governance and flexibility within its institutions regarding a risk-based approach. She said while frameworks are incredibly helpful, the NYDFS does not believe its regulation conflicts with any of the frameworks.

Director Farmer said he agrees with Superintendent Vullo’s request urging the Working Group to come up with a uniform basis. He said he does not know if it would be the New York regulation, but it is a good regulation for the Working Group to consider.

Ms. Murphy said the two instances in which the superintendent must be notified are either when notice is required to be provided to any other government agency or if the event has a reasonable likelihood of materially harming any material part of the normal operations with the covered entity. She said if the breach would harm the covered entity, then the superintendent needs to be notified, as distinct from the breach would harm consumers. Ms. Murphy asked if Superintendent Vullo had some idea about what is meant by the words “reasonable likelihood” and “material harm.” Superintendent Vullo said if a breach harms consumers, it harms the normal operations of the entity because the entity is obligated under New York law to protect the privacy of the data of the consumers, and it defines the personally identifiable information that is covered by its regulation. She said the NYDFS was trying to avoid being notified regarding every unsuccessful breach. Superintendent Vullo said the NYDFS recognizes there is a balance between receiving every possible breach and a breach that has a reasonable likelihood to cause harm.


Superintendent Dwyer said since the 2016 Fall National Meeting, the Insurance Data Security Model Law drafting group has met via conference call March 7, Feb. 21, Feb. 7, Jan. 24 and Jan. 10, 2017, and Dec. 22, 2016. The third version of the Insurance Data Security Model Law draft was released on Feb. 27, and the drafting group received numerous comments from interested stakeholders.

While there is still work to be done, there appears to be consensus regarding risk-based security requirements in the current version of the draft model law. Superintendent Dwyer said interested parties that have not yet submitted comments regarding the draft model law, or that have comments regarding Superintendent Vullo’s comments during today’s meeting, should submit their comments by close of business April 17. She said a discussion draft of the model law will be released prior to a conference call May 9 to continue discussion.

Mr. Provost said it appears there are two parts to the model law draft, the prevention and the cure. He said it appears there is little contention regarding the prevention portion of the draft model. Mr. Provost said it might be worthwhile to finish the portion of the model dealing with prevention and dealing with the cure later. Commissioner Wade agreed with these comments, as this is important work needing to be finished.

Superintendent Dwyer made a motion, seconded by Ms. Murphy, to adopt the report of the drafting group. The motion passed unanimously.

5. **Heard a Presentation from HEMISPHERE Cyber Risk Management and the ACORD**

Bill Pieroni (Association for Cooperative Operations Research and Development—ACORD) said four out of five of the top brokers, 21 of 25 of the top property/casualty (P/C) insurers, 19 out of 25 of the top life writers, 20 out of 25 reinsurers, and nine out of 10 top 5 solution providers globally use ACORD standards to enable transactions across the insurance value chain. Approximately 80% of ACORD’s members are involved with P/C insurance, while the remainder of the members are scattered between life and annuity or reinsurers.

Twenty countries represent one-third of all the premium dollars globally driven through transactions leveraging ACORD standards. In terms of data exchange, 80,000 hours are spent developing standards annually through volunteer efforts through ACORD’s members. There are 6,000 regulatory submissions in the U.S. alone. Mr. Pieroni said 300,000 forms have been downloaded over the past five years. There are 6,000,000 annual ACORD message transactions, as well as 7,000 core systems leveraging ACORD standards. ACORD sees an opportunity to increase both capacity and competency. There are
less than 60 insurers writing cyber insurance in the U.S., with a handful of these insurers driving one out of every four premium dollars.

There are not many standard offerings in the cyber insurance market, as they tend to be highly customized. Mr. Pieroni said ACORD standards could help not only with insurers entering the increasing capacity and competency in the cyber insurance market, but also could help insureds. ACORD’s cyber standards vision is to create a unified approach for cyber risk to improve data quality and align to the regulatory requirements across all 50 states.

ACORD creates data standards that are actionable and repeatable. ACORD will address market challenges by investing in assets and solutions to support regulators. Over the past five years, the compound annual growth rate of cybersecurity insurance has been growing on average of 25%. However, it is uneven among insurers, as more than 60 insurers offer stand-alone cyber insurance coverage, with the top five driving more than 25% of the market. The challenge is that there is a 3.8% adoption of cyber insurance purchases for small- to mid-size businesses and 25.9% for large firms. ACORD believes it is critically important to make sure it is removing the barriers associated with launching programs, products and services through its data standards. Mr. Pieroni said 83% of small business owners deal with trying to protect themselves against cyberattacks and have a small amount of coverage. Many of the small- to mid-size businesses cannot afford cyber insurance, and 30% of all cyber insurance claims globally exceeded policy limits. Mr. Pieroni said 33% of U.S. financial services firms have cyber insurance coverage, with an average limit of less than $25 million.

Carter Schoenberg (HEMISPHERE Cyber Risk Management) said as organizations become more interconnected, an unforeseen volume of cybersecurity insurance claims surface. Cybercrime statistics put cybercrime at 77.5%. Cyberespionage, which may arguably be included with cybercrime, is at 6.7%; Hacktivism is at 13.5%; and cyberwarfare is at 2.3%. The focus has shifted from disruption to theft and extortion, and the impact is what is driving the cyber insurance marketplace. The traditional approach has been to use technology solutions. In a recent survey, 81% of hackers interviewed said they could identify and exfiltrate data in less than 12 hours, and 88% of the respondents claimed they could compromise at a rate of less than 12 hours. The primary rationale for the NIST updates is due to the risks in the supply chain. Approximately 80% of the policy value is used in the incident response phase, which leaves only 20% of the policy value to deal with breach notifications, credit monitoring, etc.

The questionnaires given to an insured to answer questions regarding security practices vary by carrier and do not align with the current cyberthreat landscape. The insurance sector concerns include the lack of data to make better-qualified decisions during the insurance application process. ACORD suggests two core solutions, the first being Cyber Standard 2.0. This standard will be a significant addition to current standards with new breach notification forms to address evolving stakeholder needs. The standard also will be multitiered to address internal cyberrisk maturity. Secondly, industry-owned utilities, such as an Information Sharing and Analysis Organization (ISAO), are designed to develop a consortium to address new challenges in the cyber insurance market. The culmination of these proposed solutions will provide greater coordination and alignment with regulatory stakeholders to address critical industry needs. Mr. Pieroni said there are a significant number of insurers writing cyber insurance today that are engaging in writing the coverage on an ad hoc basis, which includes non-standard, manuscript policies, which is Tier 1 of the Carrier Maturity Hierarchy. Tier 2 includes insurers using technology to codify and systematize the actual assessment, underwriting, rating, pricing and issuance of the policy. Tier 3 includes technology and process, which uses key outputs and indicators married to a technology. Lastly, Tier 4 includes information technology, data, applications, architecture and internal business processes to assess the risk view, the loss cost and the organizational skillsets.

6. Discussed Other Matters

Director Farmer said the Working Group would receive surplus lines data this year along with the data included in the cybersecurity supplement. He said cyber insurance report will be presented at the Summer National Meeting.

Having no further business, the Cybersecurity (EX) Working Group adjourned.
Hear an Update Regarding Federal Cybersecurity Legislation
Attachment B

Receive a Report regarding the Data Collected from the Cybersecurity Insurance Coverage Supplement of the NAIC 2016 Property/Casualty Annual Statement and Surplus Lines Data Collection
Attachment C

Discuss the Insurance Data Security Model Law
INSURANCE DATA SECURITY MODEL LAW

Table of Contents

Section 1. Title
Section 2. Purpose and Intent
Section 3. Definitions
Section 4. Information Security Program
Section 5. Investigation of a Cybersecurity Event
Section 6. Notification of a Cybersecurity Event
Section 7. Power of Commissioner
Section 8. Confidentiality
Section 9. Exceptions
Section 10. Penalties
Section 11. Rules and Regulations [OPTIONAL]
Section 12. Severability
Section 13. Effective Date

Section 1. Title

This Act shall be known and may be cited as the “Insurance Data Security Law.”

Section 2. Purpose and Intent

A. The purpose and intent of this Act is to establish standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to Licensees, as defined in Section 3.

B. This Act may not be construed to create or imply a private cause of action for violation of its provisions nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.

Section 3. Definitions

As used in this Act, the following terms shall have these meanings:

A. “Authorized Individual” means an individual known to and screened by the Licensee and determined to be necessary and appropriate to have access to the Nonpublic Information held by the Licensee and its Information Systems.

B. “Commissioner” means the chief insurance regulatory official of the state.

C. “Consumer” means an individual, including but not limited to applicants, policyholders, insureds, beneficiaries, claimants, and certificate holders who is a resident of this State and whose Nonpublic Information is in a Licensee’s possession, custody or control.

D. “Cybersecurity Event” means an event resulting in unauthorized access to, disruption or misuse of, an Information System or information stored on such Information System.

The term “Cybersecurity Event” does not include the unauthorized acquisition of Encrypted Nonpublic Information if the encryption, process or key is not also acquired, released or used without authorization.

Cybersecurity Event does not include an event with regard to which the Licensee has determined that the Nonpublic Information accessed by an unauthorized person has not been used or released and has been returned or destroyed.
E. “Department” means the [insert name of insurance regulatory body].

F. “Encrypted” means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.

G. “Information Security Program” means the administrative, technical, and physical safeguards that a Licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle Nonpublic Information.

H. “Information System” means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems.

I. “Licensee” means any Person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State but shall not include a purchasing group or a risk retention group chartered and licensed in a state other than this State.

J. “Multi-Factor Authentication” means authentication through verification of at least two of the following types of authentication factors:

   (1) Knowledge factors, such as a password; or

   (2) Possession factors, such as a token or text message on a mobile phone; or

   (3) Inherence factors, such as a biometric characteristic.

K. “Nonpublic Information” means information that is not Publicly Available Information and is:

   (1) Business related information of a Licensee the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the Licensee;

   (2) Any information concerning a Consumer which because of name, number, personal mark, or other identifier can be used to identify such Consumer, in combination with any one or more of the following data elements:

      (a) Social Security number,

      (b) Driver’s license number or non-driver identification card number,

      (c) Account number, credit or debit card number,

      (d) Any security code, access code or password that would permit access to a Consumer’s financial account, or

      (e) Biometric records;

   (3) Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a Consumer and that relates to

      (a) The past, present or future physical, mental or behavioral health or condition of any Consumer or a member of the Consumer’s family,

      (b) The provision of health care to any Consumer, or

      (c) Payment for the provision of health care to any Consumer.
L. “Person” means any individual or any non-governmental entity, including but not limited to any non-governmental partnership, corporation, branch, agency or association.

M. “Publicly Available Information” means any information that a Licensee has a reasonable basis to believe is lawfully made available to the general public from: federal, state or local government records; widely distributed media; or disclosures to the general public that are required to be made by federal, state or local law.

For the purposes of this definition, a Licensee has a reasonable basis to believe that information is lawfully made available to the general public if the Licensee has taken steps to determine:

(1) That the information is of the type that is available to the general public; and

(2) Whether a Consumer can direct that the information not be made available to the general public and, if so, that such Consumer has not done so.

N. “Risk Assessment” means the Risk Assessment that each Licensee is required to conduct under Section 4C of this Act.

O. “State” means [adopting state].

P. “Third-Party Service Provider” means a Person, not otherwise defined as a Licensee, that contracts with a Licensee to maintain, process, store or otherwise is permitted access to Nonpublic Information through its provision of services to the Licensee.

Section 4. Information Security Program

A. Implementation of an Information Security Program

Commensurate with the size and complexity of the Licensee, the nature and scope of the Licensee’s activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee’s possession, custody or control, each Licensee shall develop, implement, and maintain a comprehensive written Information Security Program based on the Licensee’s Risk Assessment and that contains administrative, technical, and physical safeguards for the protection of Nonpublic Information and the Licensee’s Information System.

B. Objectives of Information Security Program

A Licensee’s Information Security Program shall be designed to:

(1) Protect the security and confidentiality of Nonpublic Information and the security of the Information System;

(2) Protect against any threats or hazards to the security or integrity of Nonpublic Information and the Information System;

(3) Protect against unauthorized access to or use of Nonpublic Information, and minimize the likelihood of harm to any Consumer; and

(4) Define and periodically reevaluate a schedule for retention of Nonpublic Information and a mechanism for its destruction when no longer needed.

C. Risk Assessment

The Licensee shall:

(1) Designate one or more employees, an affiliate, or an outside vendor designated to act on behalf of the Licensee who is responsible for the Information Security Program;
Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of Nonpublic Information, including the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third-Party Service Providers;

Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Nonpublic Information;

Assess the sufficiency of policies, procedures, Information Systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the Licensee’s operations, including:

(a) Employee training and management;

(b) Information Systems, including network and software design, as well as information classification, governance, processing, storage, transmission, and disposal; and

(c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and

Implement information safeguards to manage the threats identified in its ongoing assessment, and no less than annually, assess the effectiveness of the safeguards’ key controls, systems, and procedures. A summary of this assessment shall be included in the annual report required by Section 4I.

D. Risk Management

Based on its Risk Assessment, the Licensee shall:

Design its Information Security Program to mitigate the identified risks, commensurate with the size and complexity of the Licensee’s activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee’s possession, custody or control.

Determine which security measures listed below are appropriate to implement. In making this determination, the Licensee shall use the best practices for cybersecurity protection, detection, and remediation available commensurate with the size and complexity of the Licensee’s activities, including its use of Third-Party Service Providers, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee’s possession, custody or control.

(a) Place access controls on Information Systems, including controls to authenticate and permit access only to Authorized Individuals to protect against the unauthorized acquisition of Nonpublic Information;

(b) Identify and manage the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization’s risk strategy;

(c) Restrict access at physical locations containing Nonpublic Information, only to Authorized Individuals;

(d) Protect by encryption or other appropriate means, all Nonpublic Information while being transmitted over an external network and all Nonpublic Information stored on a laptop computer or other portable computing or storage device or media;

(e) Adopt secure development practices for in-house developed applications utilized by the Licensee and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Licensee;
(f) Modify the Information System in accordance with the Licensee’s Information Security Program;

(g) Utilize effective controls, which may include Multi-Factor Authentication procedures for any individual accessing Nonpublic Information;

(h) Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, Information Systems;

(i) Include audit trails within the Information Security Program designed to detect and respond to Cybersecurity Events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the Licensee;

(j) Implement measures to protect against destruction, loss, or damage of Nonpublic Information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and

(k) Develop, implement, and maintain procedures for the secure disposal of Nonpublic Information in any format.

(3) Include cybersecurity risks in the Licensee’s enterprise risk management process.

(4) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and

(5) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the Licensee in the Risk Assessment.

E. Oversight by Board of Directors

If the Licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

(1) Require the Licensee’s executive management or its delegates to develop, implement, and maintain the Licensee’s Information Security Program;

(2) Require the Licensee’s executive management or its delegates to report in writing at least annually, the following information:

(a) The overall status of the Information Security Program and the Licensee’s compliance with this Act; and

(b) Material matters related to the Information Security Program, addressing issues such as risk assessment, risk management and control decisions, Third-Party Service Provider arrangements, results of testing, Cybersecurity Events or violations and management’s responses thereto, and recommendations for changes in the Information Security Program.

(3) If executive management delegates any of its responsibilities under Section 4 of this Act, it shall oversee the development, implementation and maintenance of the Licensee’s Information Security Program prepared by the delegate(s) and shall receive a report from the delegate(s) complying with the requirements of the report to the Board of Directors above.
F. Oversight of Third-Party Service Provider Arrangements

(1) Each Licensee shall implement written policies and procedures designed to ensure the security of Information Systems and Nonpublic Information that are accessible to, or held by, Third-Party Service Providers. Such policies and procedures shall be based on the Risk Assessment of the Licensee and shall address to the extent applicable:

(a) The identification and risk assessment of Third-Party Service Providers;

(b) Minimum cybersecurity practices required to be met by such Third-Party Service Providers in order for them to do business with the Licensee;

(c) Due diligence processes used to evaluate the adequacy of cybersecurity practices of such Third-Party Service Providers; and

(d) Periodic assessment of such Third-Party Service Providers based on the risk they present and the continued adequacy of their cybersecurity practices.

(2) Such policies and procedures shall include relevant guidelines for due diligence and/or contractual protections relating to Third-Party Service Providers including, to the extent applicable, guidelines addressing:

(a) The Third-Party Service Provider’s policies and procedures for access controls, including its use of Multi-Factor Authentication, to limit access to relevant Information Systems and Nonpublic Information;

(b) The Third-Party Service Provider’s policies and procedures for use of Encryption to protect Nonpublic Information in transit and at rest;

(c) Notice to be provided to the Licensee in the event of a Cybersecurity Event directly impacting the Licensee’s Information Systems or Nonpublic Information being held by the Third-Party Service Provider; and

(d) Representations and warranties addressing the Third-Party Service Provider’s cybersecurity policies and procedures that relate to the security of the Licensee’s Information Systems or Nonpublic Information.

G. Program Adjustments

The Licensee shall monitor, evaluate and adjust, as appropriate, the Information Security Program consistent with any relevant changes in technology, the sensitivity of its Nonpublic Information, internal or external threats to information, and the Licensee’s own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to Information Systems.

H. Incident Response Plan

(1) As part of its Information Security Program, each Licensee shall establish a written incident response plan designed to promptly respond to, and recover from, any Cybersecurity Event that compromises the confidentiality, integrity or availability of Nonpublic Information in its possession, the Licensee’s Information Systems, or the continuing functionality of any aspect of the Licensee’s business or operations.

(2) Such incident response plan shall address the following areas:

(a) The internal process for responding to a Cybersecurity Event;

(b) The goals of the incident response plan;
(c) The definition of clear roles, responsibilities and levels of decision-making authority;

(d) External and internal communications and information sharing;

(e) Identification of requirements for the remediation of any identified weaknesses in Information Systems and associated controls;

(f) Documentation and reporting regarding Cybersecurity Events and related incident response activities; and

(g) The evaluation and revision as necessary of the incident response plan following a Cybersecurity Event.

I. Annual Report to Commissioner of Domiciliary State

Upon the Commissioner’s request, and no more than once each year, each insurer domiciled in this State shall file an annual written report with the Commissioner. The report, which may reference or incorporate other filings with any other state, federal, and international regulatory agencies, shall summarize the assessment mandated by Subsection 4C(5) above and any areas, systems or processes that require material improvement, updating or redesign. The insurer shall document the remedial efforts planned and underway to address such areas, systems or processes. Such documentation shall be available for inspection by the Commissioner.

Drafting Note: In order to ensure that the Commissioner is receiving the most current information from an insurer, Section 4I recognizes that the time for filing the Annual Report during the calendar year may vary from insurer to insurer, depending on the timing of the insurer’s assessment. In any event, the report shall be filed once each year, with the insurer apprising the Commissioner as to the anticipated time of filing.

Section 5. Investigation of a Cybersecurity Event

A. If the Licensee learns that a Cybersecurity Event has or may have occurred the Licensee, or an outside vendor and/or service provider designated to act on behalf of the Licensee, shall conduct a prompt investigation.

B. During the investigation, the Licensee, or an outside vendor and/or service provider designated to act on behalf of the Licensee, shall, at a minimum determine as much of the following information as possible:

   (1) Determine whether a Cybersecurity Event has occurred;

   (2) Assess the nature and scope of the Cybersecurity Event;

   (3) Identify any Nonpublic Information that may have been involved in the Cybersecurity Event; and

   (4) Perform or oversee reasonable measures to restore the security of the Information Systems compromised in the Cybersecurity Event in order to prevent further unauthorized acquisition, release or use of Nonpublic Information in the Licensee's possession, custody or control.

C. If the Licensee learns that a Cybersecurity Event has or may have occurred in a system maintained by a Third-Party Service Provider, the Licensee will complete the steps listed in Section 5B above or confirm and document that the Third-Party Service Provider has completed those steps.

D. The Licensee shall maintain records concerning all Cybersecurity Events for a period of at least five years from the date of the Cybersecurity Event and shall produce those records upon demand of the Commissioner.

Section 6. Notification of a Cybersecurity Event

A. Notification to the Commissioner

Each Licensee shall notify the Commissioner as promptly as possible but in no event later than 72 hours from a determination that a Cybersecurity Event has occurred if:
(1) This State is the Licensee’s state of domicile, in the case of an insurer, or this State is the Licensee’s home state, in the case of a producer, as those terms are defined in [insert reference to Producer Licensing Model Act]; or

(2) The Licensee reasonably believes that the Nonpublic Information involved is of 250 or more Consumers residing in this State and that is either of the following:

   (a) A Cybersecurity Event impacting the Licensee of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body pursuant to any state or federal law; or

   (b) A Cybersecurity Event that has a reasonable likelihood of materially harming:

      (i) Any Consumer residing in this State; or

      (ii) Any material part of the normal operation(s) of the Licensee.

B. The Licensee shall provide as much of the following information as possible. The Licensee shall provide the information in electronic form as directed by the Commissioner. The Licensee shall have a continuing obligation to update and supplement initial and subsequent notifications to the Commissioner concerning the Cybersecurity Event.

   (1) Date of the Cybersecurity Event;

   (2) Description of how the information was exposed, lost, stolen, or breached, including the specific roles and responsibilities of Third-Party Service Providers, if any;

   (3) How the Cybersecurity Event was discovered;

   (4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done;

   (5) The identity of the source of the Cybersecurity Event;

   (6) Whether Licensee has filed a police report or has notified any regulatory, government or law enforcement agencies and, if so, when such notification was provided;

   (7) Description of the specific types of information acquired without authorization. Specific types of information means particular data elements including, for example, types of medical information, types of financial information or types of information allowing identification of the Consumer;

   (8) The period during which the Information System was compromised by the Cybersecurity Event;

   (9) The number of total Consumers in this State affected by the Cybersecurity Event. The Licensee shall provide the best estimate in the initial report to the Commissioner and update this estimate with each subsequent report to the Commissioner pursuant to this section;

   (10) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls or internal procedures were followed;

   (11) Description of efforts being undertaken to remediate the situation which permitted the Cybersecurity Event to occur;

   (12) A copy of the Licensee’s privacy policy and a statement outlining the steps the Licensee will take to investigate and notify Consumers affected by the Cybersecurity Event; and
(13) Name of a contact person who is both familiar with the Cybersecurity Event and authorized to act for the Licensee.

C. Notification to Consumers. Licensee shall comply with [insert state’s data breach notification law], as applicable, and provide a copy of the notice sent to Consumers under that statute to the Commissioner, when a Licensee is required to notify the Commissioner under Section 6A.

D. Notice Regarding Cybersecurity Events of Third-Party Service Providers

(1) In the case of a Cybersecurity Event in a system maintained by a Third-Party Service Provider, of which the Licensee has become aware, the Licensee shall treat such event as it would under Section 6A.

(2) The computation of Licensee’s deadlines shall begin on the day after the Third-Party Service Provider notifies the Licensee of the Cybersecurity Event or the Licensee otherwise has actual knowledge of the Cybersecurity Event, whichever is sooner.

(3) Nothing in this Act shall prevent or abrogate an agreement between a Licensee and another Licensee, a Third-Party Service Provider or any other party to fulfill any of the investigation requirements imposed under Section 5 or notice requirements imposed under Section 6.

E. Notice Regarding Cybersecurity Events of Reinsurers to Insurers

(1) (a) In the case of a Cybersecurity Event involving Nonpublic Information that is used by the Licensee that is acting as an assuming insurer or in the possession, custody or control of a Licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected Consumers, the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of making the determination that a Cybersecurity Event has occurred.

(b) The ceding insurers that have a direct contractual relationship with affected Consumers shall fulfill the consumer notification requirements imposed under [insert the state’s breach notification law] and any other notification requirements relating to a Cybersecurity Event imposed under Section 6.

(2) (a) In the case of a Cybersecurity Event involving Nonpublic Information that is in the possession, custody or control of a Third-Party Service Provider of a Licensee that is an assuming insurer, the assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of receiving notice from its Third-Party Service Provider that a Cybersecurity Event has occurred.

(b) The ceding insurers that have a direct contractual relationship with affected Consumers shall fulfill the consumer notification requirements imposed under [insert the state’s breach notification law] and any other notification requirements relating to a Cybersecurity Event imposed under Section 6.

F. Notice Regarding Cybersecurity Events of Insurers to Producers of Record

In the case of a Cybersecurity Event involving Nonpublic Information that is in the possession, custody or control of a Licensee that is an insurer or its Third-Party Service Provider and for which a Consumer accessed the insurer’s services through an independent insurance producer, the insurer shall notify the producers of record of all affected Consumers within 72 hours of making the determination that a Cybersecurity Event has occurred.

The insurer is excused from this obligation for those instances in which it does not have the current producer of record information for any individual Consumer.
Section 7. Power of Commissioner

A. The Commissioner shall have power to examine and investigate into the affairs of any Licensee to determine whether the Licensee has been or is engaged in any conduct in violation of this Act. This power is in addition to the powers which the Commissioner has under [insert applicable statutes governing the investigation or examination of insurers]. Any such investigation or examination shall be conducted pursuant to [insert applicable statutes governing the investigation or examination of insurers].

B. Whenever the Commissioner has reason to believe that a Licensee has been or is engaged in conduct in this State which violates this Act, the Commissioner may take action that is necessary or appropriate to enforce the provisions of this Act.

Section 8. Confidentiality

A. Any documents, materials or other information in the control or possession of the Department that are furnished by a Licensee or an employee or agent thereof acting on behalf of Licensee pursuant to Section 4I, Section 6B(2), (3), (4), (5), (8), (10), and (11), or that are obtained by the Commissioner in an investigation or examination pursuant to Section 7 of this Act shall be confidential by law and privileged, shall not be subject to [insert reference to state open records, freedom of information, sunshine or other appropriate law], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the Commissioner is authorized to use the documents, materials or other information in the furtherance of any regulatory or legal action brought as a part of the Commissioner’s duties.

B. Neither the Commissioner nor any person who received documents, materials or other information while acting under the authority of the Commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to Section 8A.

C. In order to assist in the performance of the Commissioner’s duties under this Act, the Commissioner:

(1) May share documents, materials or other information, including the confidential and privileged documents, materials or information subject to Section 8A, with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees in writing to maintain the confidentiality and privileged status of the document, material or other information;

(2) May receive documents, materials or information, including otherwise confidential and privileged documents, materials or information, from the National Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material or information; and

(3) May enter into agreements governing sharing and use of information consistent with this subsection.

D. No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the Commissioner under this section or as a result of sharing as authorized in Section 8C.

E. Nothing in this Act shall prohibit the Commissioner from releasing final, adjudicated actions that are open to public inspection pursuant to [insert appropriate reference to state law] to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries.

Drafting Note: States conducting an investigation or examination under their examination law may apply the confidentiality protections of that law to such an investigation or examination.
Section 9. Exceptions

A. The following exceptions shall apply to this Act:

(1) A Licensee with fewer than ten employees, including any independent contractors, is exempt from Section 4 of this Act;

(2) A Licensee subject to Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996 (Health Insurance Portability and Accountability Act) that has established and maintains an Information Security Program pursuant to such statutes, or rules, regulations, procedures or guidelines established thereunder, will be considered to meet the requirements of Section 4, provided that Licensee can produce, upon request, documentation satisfactory to the Commissioner that independently validates such compliance;

(3) An employee, agent, representative or designee of a Licensee, who is also a Licensee, is exempt from Section 4 and need not develop its own Information Security Program to the extent that the employee, agent, representative or designee is covered by the Information Security Program of the other Licensee.

B. In the event that a Licensee ceases to qualify for an exception, such Licensee shall have 180 days to comply with this Act.

Section 10. Penalties

In the case of a violation of this Act, a Licensee may be penalized in accordance with [insert general penalty statute].

Section 11. Rules and Regulations [OPTIONAL]

The Commissioner may, in accordance with [the state statute setting forth the ability of the Department to adopt regulations] issue such regulations as shall be necessary to carry out the provisions of this Act.

Drafting Note: This provision is applicable only to states requiring this language.

Section 12. Severability

If any provisions of this Act or the application thereof to any person or circumstance is for any reason held to be invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected thereby.

Section 13. Effective Date

This Act shall take effect on [insert a date]. Licensees shall have one year from the effective date of this Act to implement Section 4 of this Act and two years from the effective date of this Act to implement Section 4F of this Act.
Consider Adoption of the Insurance Data Security Model Law
Any Other Matters