THE COUNCIL
The Council of Insurance Agents & Brokers

Steptoe

***DRAFT – August 24, 2020***

# *State Data Security Framework Survey*

- The NAIC Data Security Model Law ("NAIC Model Law") establishes a framework of generally accepted best practices in information security, as well as a legal framework for requiring insurers and producers to implement such programs.

- Outlined below is a comprehensive overview of state laws and their composition relative to the NAIC Model Law. To date, ten states—Alabama, Connecticut, Delaware, Indiana, Michigan, Mississippi, New Hampshire, Ohio, South Carolina, and Virginia—have enacted laws that align with the NAIC Model Law. Maryland and New York have enacted their own, distinct data security provisions.

- Though many states vary in their implementation of the NAIC Model Law (and the specific contours and details of their provisions), most states have incorporated its general framework, including requirements governing:

  - The development/implementation of a written "Information Security Program" (ISP),

  - The contours of an investigation into a cybersecurity event,

  - Notification of the state insurance regulator following a determination that a cybersecurity event has occurred, and

  - Certain limited exceptions.

- The below survey outlines the varying state approaches to enacting the NAIC Model Law via a comparison of existing statutory text, associated regulatory provisions, and interpretive administrative guidance with respect to these specific provisions. It does not include penalty structures, a complete analysis of the definitional provisions, or discussion of the state regulator's authority.

- We envision this survey to be an evergreen document. As updates are put forth—whether through legislative or administrative action—we will update the document and provide a brief overview of the relevant changes in this top box in ***bold and italicized blue text***. We ask, therefore, that you continuously review the document for updates to any statutes, regulations, bulletins, or other guidance documents. That said, if you see laws enacted, regulations finalized, bulletins issued, or enforcement actions undertaken that are not reflected in this survey, please let us know.

| State | ISP Requirements | Investigation Requirements | Notification Requirements | Exceptions | Other |
|---|---|---|---|---|---|
| ***NAIC Model Law*** | Requires implementation of a written ISP (as overseen by the board of directors), details its objectives, and dictates how the ISP should be developed.<br>Requires licensees to undertake a risk assessment and then design their ISPs so as to mitigate the identified risks, including a determination as to whether certain security measures (e.g., placement of access controls, identification and management of data, restriction of access at physical locations, etc.) are appropriate given the risks identified.<br>Further requires:<br>• Due diligence and oversight of third-party service providers (TPSP).<br>• Implementation of program adjustments, as needed.<br>• Establishment of an incident response plan that addresses—among other things—the internal processes for responding to/recovering from a cybersecurity event.<br>• Submission of an annual certification of compliance to the state regulator by February 15. | If the licensee learns/determines that a cybersecurity event has occurred, requires the licensee (or an outside vendor) to conduct a prompt investigation to:<br>• Determine whether a cybersecurity event occurred.<br>• Assess the nature and scope of the event.<br>• Identify any nonpublic information that may have been involved.<br>• Perform and oversee reasonable measures to restore security. | Once it is determined that a cybersecurity event has occurred, requires each licensee to notify the state regulator within 72 hours that either of the following criteria has been met:<br>• The state is the licensee's home state or<br>• The licensee reasonably believes that the nonpublic information involved affects over 250 resident-consumers and is either (1) a cybersecurity event impacting the licensee of which notice is required to be provided pursuant to state/federal law or (2) a cybersecurity event that has a reasonable likelihood of materially harming any consumer in the state or any material part of the licensee's normal operations.<br>Dictates the information that must be provided to the Commissioner (e.g., the date of the cybersecurity event, a description of how the information was exposed/breached, how the event was discovered, etc.); requires notification to consumers comport with the state's data breach notification law; addresses how notice should be handled if the cybersecurity event occurs in a system maintained by a TPSP, etc. | Sets forth three primary exceptions which, if applicable, exempt licensees from the requirement that they develop and implement an ISP. These exemptions apply to:<br>• Licensees with fewer than 10 employees.<br>• Licensees subject to HIPAA that have established and currently maintain an ISP pursuant to such statutes, rules, regulations, guidelines, etc., provided the licensee submits a written statement certifying its compliance with the state regulator.<br>• An employee, agent, representative, or designee of a licensee (i.e., such individuals need not develop their own ISPs to the extent that they are covered by the licensee's ISP). | N/A |

| State | ISP Requirements | Investigation Requirements | Notification Requirements | Exceptions | Other |
|---|---|---|---|---|---|
| ***Alabama***<br>Ala. Code §§ 27-62-1 et seq. | Mirrors the NAIC Model Law, except does not require licensees to consider implementing security procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee.<br>Sets a state-specific deadline, giving licensees until ***May 1, 2021*** to comply with the requirements relating to a licensee's due diligence and oversight of TPSPs. | MIRRORS NAIC MODEL LAW | Mirrors the NAIC Model Law, except:<br>• Requires notification of the state regulator within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred.<br>• Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Alabama and the breach has a "reasonable likelihood" of harming a resident or the licensee's normal operations).<br>• Requires licensees to notify the Commissioner if a TPSP is breached, unless the TPSP provides the required notice to the Commissioner. | Expands exemptions in the NAIC Model Law to include those with:<br>• Fewer than 25 employees (rather than 10).<br>• Less than $5 million in gross annual revenue.<br>• Less than $10 million in year-end total assets.<br>• ISPs in accordance with GLBA. | Unlike the NAIC Model Law, does not include in the definition of "nonpublic information" "business related information" the tampering of which would cause a material adverse impact to the licensee. |
| ***Alaska*** | | | | | |
| ***Arizona*** | | | | | |
| ***Arkansas*** | | | | | |
| ***California*** | | | | | |
| ***Colorado*** | | | | | |
| ***Connecticut***<br>Conn. Gen. Stat. § 38a-38 | Mirrors the NAIC Model Law, except sets two state-specific deadlines:<br>• Gives licensees until ***October 1, 2020*** to develop, implement, and maintain an ISP.<br>• Gives licensees until ***October 1, 2021*** to comply | MIRRORS NAIC MODEL LAW | Mirrors the NAIC Model Law, except:<br>• Requires notification of the state regulator within 3 business days (rather than 72 hours) of a cybersecurity event (rather than from the determination that a cybersecurity event occurred).<br>• Establishes more specific criteria to trigger notification to the state | Expands exemptions in the NAIC Model Law to include those with:<br>• ***Before October 1, 2021***, fewer than 20 employees (rather than 10, which will take effect ***on October 1, 2021***). | N/A |

| State | ISP Requirements | Investigation Requirements | Notification Requirements | Exceptions | Other |
|---|---|---|---|---|---|
| | with the requirements relating to a licensee's due diligence and oversight of TPSPs. | | regulator (i.e., requires notification if the licensee is licensed in Connecticut and 250+ residents are affected). | • ISPs in accordance with statutes, rules, and regulations of a jurisdiction approved by the state regulator (e.g., compliance with NYDFS' cybersecurity regulation), though an annual statement certifying compliance must be filed with the state regulator. | |
| ***Delaware***<br>Del. Code Ann. §§ 8601 et seq. | MIRRORS NAIC MODEL LAW | MIRRORS NAIC MODEL LAW | Mirrors the NAIC Model Law, except:<br>• Requires notification of the state regulator within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred.<br>• Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Delaware and the cybersecurity event results in a reasonable likelihood of materially harming consumers, a reasonable likelihood of materially harming any material part of the licensee's normal operations, or the licensee is required to provide notice to a government, agency, or other body under state or federal law). | Expands exemptions in the NAIC Model Law to include those with fewer than 15 employees (rather than 10). | N/A |

| State | ISP Requirements | Investigation Requirements | Notification Requirements | Exceptions | Other |
|---|---|---|---|---|---|
| | | | - Imposes industry-specific requirements governing consumer notice (e.g., notification within 60 days unless certain exceptions are met, appropriate forms of notice, etc.). | | |
| ***D.C.*** | | | | | |
| ***Florida*** | | | | | |
| ***Georgia*** | | | | | |
| ***Hawaii*** | | | | | |
| ***Idaho*** | | | | | |
| ***Illinois*** | | | | | |
| ***Indiana*** | Mirrors the NAIC Model Law, except:<br>- Does not require licensees to consider implementing security procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee.<br>- Does not affirmatively require the licensee to adjust the ISP.<br>Like the NAIC Model Law, requires annual certification to the state regulator, but such certification must be submitted by April 15 (rather than February 15). | MIRRORS NAIC MODEL LAW | Mirrors the NAIC Model Law, except:<br>- Requires notification of the state regulator within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred.<br>- Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Indiana and the cybersecurity event has a reasonable likelihood of materially harming a consumer residing in Indiana or any material part of the normal operations of the licensee).<br>- Does not contain language dictating how notice should be given regarding cybersecurity events of TPSPs. | Expands exemptions in the NAIC Model Law to include those with:<br>- Fewer than 50 employees (rather than 10).<br>- Less than $5 million in gross annual revenue.<br>- Less than $10 million in year-end total assets.<br>- ISPs in accordance with GLBA.<br>Does not apply to financial institutions as defined under federal law. | Entitles compliant licensees to an affirmative defense to any tort action that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning nonpublic information. |
| ***Iowa*** | | | | | |

| State | ISP Requirements | Investigation Requirements | Notification Requirements | Exceptions | Other |
|---|---|---|---|---|---|
| ***Kansas*** | | | | | |
| ***Kentucky*** | | | | | |
| ***Louisiana*** | | | | | |
| ***Maine*** | | | | | |
| ***Maryland***<br>Md. Ins. Code § 4-406(b); Md. Bus. Code § 14-3504; Bulletin 19-14 | | | Does not mirror the NAIC Model Law.<br>Requires carriers to notify the state regulator within 45 days of determining that a breach occurred if the carrier:<br>• Conducts an investigation required under the state's data breach notification law; and<br>• Determines that the breach creates a likelihood that personal information has been or will be misused. | | |
| ***Massachusetts*** | | | | | |
| ***Michigan***<br>Mich. Code Ann. §§ 553 et seq.<br>***Effective January 20, 2021*** | Mirrors the NAIC Model Law, except sets two state-specific deadlines:<br>• Gives licensees until ***January 20, 2022*** to develop, implement, and maintain an ISP.<br>• Gives licensees until ***January 20, 2023*** to comply with the requirements relating to a licensee's due diligence and oversight of TPSPs. | Mirrors the NAIC Model Law, except does not contain language governing how a licensee should respond if they learn that a cybersecurity event has occurred in a system maintained by a TPSP. | Mirrors the NAIC Model Law, except:<br>• Requires notification of the state regulator within 10 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred.<br>• Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Michigan and the cybersecurity event has a reasonable likelihood of materially harming consumers or the licensee's normal operations). | Expands exemptions in the NAIC Model Law to include those with fewer than 25 employees (rather than 10). | Clarifies that a cybersecurity event will not be deemed to have occurred in the event of unauthorized access by a person who acted in good faith and the access was related to the person's activities. |

| State | ISP Requirements | Investigation Requirements | Notification Requirements | Exceptions | Other |
|---|---|---|---|---|---|
| | | | • Imposes industry-specific requirements governing notification to consumers (e.g., dictates appropriate forms of notice). | | |
| ***Minnesota*** | | | | | |
| ***Mississippi***<br>Miss. Stat. §§ 83-5801 et seq. | Mirrors the NAIC Model Law, except does not require licensees to consider implementing security procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee. | MIRRORS NAIC MODEL LAW | Mirrors the NAIC Model Law, except:<br>• Requires notification of the Commissioner within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred.<br>• Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Mississippi and the cybersecurity event has a reasonable likelihood of materially harming consumers residing in Mississippi or the licensee's normal operations). | Expands exemptions in the NAIC Model Law to include those with:<br>• Fewer than 50 employees (rather than 10).<br>• Less than $5 million in gross annual revenue.<br>• Less than $10 million in year-end total assets.<br>• Producer and adjuster licenses<br>from the ISP requirements and the investigation and notice requirements (but only to the extent they concern cybersecurity events at TPSPs).<br>Exempts licensees affiliated with a depository institution that maintains an ISP in accordance with GLBA from the ISP requirements. | N/A |

| State | ISP Requirements | Investigation Requirements | Notification Requirements | Exceptions | Other |
|---|---|---|---|---|---|
| ***Missouri*** | | | | | |
| ***Montana*** | | | | | |
| ***Nebraska*** | | | | | |
| ***Nevada*** | | | | | |
| ***New Hampshire***<br>N.H. Rev. Stat. §§ 420-P:1 et seq. | Mirrors the NAIC Model Law, except does not require licensees to consider implementing security procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee.<br>Like the NAIC Model Law, requires annual certification to the state regulator, but such certification must be submitted by March 1 (rather than February 15). | MIRRORS NAIC MODEL LAW | Mirrors the NAIC Model Law, except:<br>• Requires notification of the Commissioner within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred.<br>• Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in New Hampshire and the cybersecurity event has a reasonable likelihood of materially harming consumers residing in New Hampshire or the licensee's normal operations). | Expands exemptions in the NAIC Model Law to include:<br>• Licensees with fewer than 20 employees (rather than 10).<br>• Licensees operating in compliance with New York's cybersecurity regulation.<br>• Continuing care retirement communities.<br>• Life settlement providers.<br>• Licensees that are banks or credit unions and that maintain an ISP in accordance with GLBA.<br>• Motor vehicle retail sellers/sales finance company.<br>• "Vendors" engaged in the sale of portable electronics insurance. | Unlike the NAIC Model Law, does not include in the definition of "nonpublic information" "business related information" the tampering of which would cause a material adverse impact to the licensee. |
| ***New Jersey*** | | | | | |
| ***New Mexico*** | | | | | |

| State | ISP Requirements | Investigation Requirements | Notification Requirements | Exceptions | Other |
|---|---|---|---|---|---|
| ***New York***<br>23 NYCCR 500<br>***Note, the New York rules pre-date the NAIC Model Law*** | Requires implementation of a "Cybersecurity Program" and dictates its "core cybersecurity functions" (e.g., identifying and assessing internal and external cybersecurity risks, using defensive infrastructure to protect the licensee's information systems, detecting cybersecurity events, etc.).<br>Requires implementation and maintenance of a written "Cybersecurity Policy" based on the licensee's risk assessment that addresses information security, data governance and classification, asset inventory and device management, etc.<br>Like the NAIC Model Law, requires the Cybersecurity Program to:<br>• Be based on a risk assessment.<br>• Include continuous monitoring, penetration testing, or vulnerability assessments; include audit trails designed to detect and respond to cybersecurity events; limit access privileges; address the secure disposal of information, etc. | N/A | Requires notification of the state regulator within 72 hours of a determination that a cybersecurity event has occurred that is either:<br>• A cybersecurity event impacting the licensee for which notice is required to be provided to any government, self-regulatory agency, or other supervisory body; or<br>• A cybersecurity event that has a reasonable likelihood of materially harming any material part of the normal operations of the licensee. | Offers several exemptions (to varying sections) for:<br>• Licensees with fewer than 10 employees located in New York.<br>• Licensees with less than $5 million in gross annual revenue in each of the last three fiscal years from New York business operations.<br>• Licensees with less than $10 million in year-end total assets.<br>• Employees, agents, representatives or designees of licensees.<br>• Licensees that do not directly/indirectly operate, maintain, utilize, or control any information systems.<br>• Licensees that do not directly/indirectly control, own, access, etc. nonpublic information.<br>Requires licensees that qualify for exemptions to file a Notice of Exemption. | Requires designation of a "Chief Information Security Officer" to oversee and implement the Cybersecurity Program, report annually to the licensee's board of directors, etc.<br>Requires the licensee to utilize qualified cybersecurity personnel to manage their cybersecurity risks/oversee the core cybersecurity functions.<br>Unlike the NAIC Model Law, provides for specific requirements concerning TPSP security policies. |

| State | ISP Requirements | Investigation Requirements | Notification Requirements | Exceptions | Other |
|---|---|---|---|---|---|
|  | • Establish a written incident response plan.<br>• Submit an annual certification to the state regulator by February 15.<br>Unlike the NAIC Model Law, requires the Cybersecurity Program to include written procedures, guidelines, etc. to ensure the use of secure development practices for in-house developed applications. |  |  |  |  |
| ***North Carolina*** |  |  |  |  |  |
| ***North Dakota*** |  |  |  |  |  |
| ***Ohio***<br>Ohio Rev. Stat. §§ 3965.01 et seq. | With respect to the annual certification, permits an insurer domiciled in Ohio and licensed exclusively to conduct business in Ohio (and no other state) to submit a written statement to the state regulator certifying that the insurer is in compliance with the ISP requirements as part of their corporate governance annual disclosure.<br>Provides that a licensee that is compliant with the ISP requirements will be deemed to have implemented a cybersecurity program that "reasonably conforms to an industry-recognized | MIRRORS NAIC MODEL LAW | Mirrors the NAIC Model Law, except requires notification of the Commissioner within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred.<br>Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Ohio and the cybersecurity event has a reasonable likelihood of materially harming a consumer or a material part of the normal operations of the license). | Mirrors the NAIC Model Law, except expands exemptions to include those with:<br>• Fewer than 20 employees (rather than 10).<br>• Less than $5 million in gross annual revenue.<br>• Less than $10 million in year-end total assets.<br>• ISPs in accordance with GLBA. | Entitles compliant licensees to an affirmative defense to any tort action that alleges that the failure to implement reasonable information security controls resulted in a data breach concerning nonpublic information. |

| State | ISP Requirements | Investigation Requirements | Notification Requirements | Exceptions | Other |
|---|---|---|---|---|---|
| | cybersecurity framework" for the purposes of the state's Uniform Commercial Code. | | | | |
| ***Oklahoma*** | | | | | |
| ***Oregon*** | | | | | |
| ***Pennsylvania*** | | | | | |
| ***Rhode Island*** | | | | | |
| ***South Carolina***<br>S.C. Code Ann. §§ 38-99-10 et seq. | MIRRORS NAIC MODEL LAW | MIRRORS NAIC MODEL LAW | MIRRORS NAIC MODEL LAW | MIRRORS NAIC MODEL LAW | N/A |
| ***South Dakota*** | | | | | |
| ***Tennessee*** | | | | | |
| ***Texas*** | | | | | |
| ***Utah*** | | | | | |
| ***Vermont*** | | | | | |
| ***Virginia***<br>Va. Code Ann. §§ 38.2-621 et seq. | Deviates from the NAIC Model Law in that it does not require the licensee to undertake certain steps with respect to the risk assessment (e.g., does not require identification of reasonably foreseeable internal or external threats; assessment of the likelihood and potential damage of the threats; assessment of the sufficiency of policies, procedures, and other safeguards in place to manage these threats, etc.). | MIRRORS NAIC MODEL LAW | Mirrors the NAIC Model Law, except requires notification of the Commissioner within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred.<br>Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Ohio and "the cybersecurity event meets threshold and other requirements prescribed by the Commissioner"; does not require the cybersecurity | Mirrors the NAIC Model Law, except expands exemptions to include those with ISPs in accordance with GLBA and does not include an exemption for small businesses (i.e., those with fewer than 10 employees). | Includes within the definition of "non-public information" a consumers' passport number or military identification number. |

| State | ISP Requirements | Investigation Requirements | Notification Requirements | Exceptions | Other |
|---|---|---|---|---|---|
| | Does not permit the licensee to determine which security measures to implement (i.e., mandates specific security measures, rather than enumerating several options).<br><br>Sets two state-specific deadlines:<br>• Gives licensees until ***January 1, 2023*** to comply with the annual certification requirement.<br>• Gives licensees until ***July 1, 2022*** to comply with the requirements relating to a licensee's due diligence and oversight of TPSPs. | | event to have a reasonable likelihood of materially harming consumers or the licensee's normal operations).<br><br>Imposes industry-specific requirements governing notification to consumers (e.g., dictates appropriate forms of notice). | | |
| ***Washington*** | | | | | |
| ***West Virginia*** | | | | | |
| ***Wisconsin*** | | | | | |
| ***Wyoming*** | | | | | |