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, eleven states—Alabama, Connecticut, Delaware, Indiana, Louisiana, 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.
- ***Please note, we have compiled more detailed analyses on specific questions raised by Council members on how states have implemented the NAIC Model Law. In particular, we have reviewed the application of the attestation requirements and certain exceptions. To the extent that such materials are of interest, they can be found at the close of this survey. See Appendix 1: Application of NAIC Model Law Attestation Requirements and Exceptions.***

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. 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. Further requires: • Due diligence and oversight of third-party service providers (TPSP). • Implementation of program adjustments, as needed. • Establishment of an incident response plan that addresses—among other things—the internal processes for responding to/recovering from a cybersecurity event. • 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: • Determine whether a cybersecurity event occurred. • Assess the nature and scope of the event. • Identify any nonpublic information that may have been involved. • 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: • The state is the licensee's home state or • 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. 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: • Licensees with fewer than 10 employees. • 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. • 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 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. 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: • Requires notification of the state regulator within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred. • 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). • 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: • Fewer than 25 employees (rather than 10). • Less than $5 million in gross annual revenue. • Less than $10 million in year-end total assets. • 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 Conn. Gen. Stat. § 38a-38	Mirrors the NAIC Model Law, except sets two state-specific deadlines: • Gives licensees until ***October 1, 2020*** to develop, implement, and maintain an ISP. • Gives licensees until ***October 1, 2021*** to comply	MIRRORS NAIC MODEL LAW	Mirrors the NAIC Model Law, except: • 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). • Establishes more specific criteria to trigger notification to the state	Expands exemptions in the NAIC Model Law to include those with: • ***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 Del. Code Ann. §§ 8601 et seq.	MIRRORS NAIC MODEL LAW	MIRRORS NAIC MODEL LAW	Mirrors the NAIC Model Law, except: • Requires notification of the state regulator within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred. • 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: • Does <u>not</u> require licensees to consider implementing security procedures for evaluating, assessing, or testing the security of externally developed applications utilized by the licensee. • Does <u>not</u> affirmatively require the licensee to adjust the ISP. 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: • Requires notification of the state regulator within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred. • Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Indiana <u>and</u> 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). • Does <u>not</u> contain language dictating how notice should be given regarding cybersecurity events of TPSPs.	Expands exemptions in the NAIC Model Law to include those with: • Fewer than 50 employees (rather than 10). • Less than $5 million in gross annual revenue. • Less than $10 million in year-end total assets. • ISPs in accordance with GLBA. Does <u>not</u> 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 La. Rev. Stat. §§ 22:2501 et seq.	Mirrors the NAIC Model Law, except sets two state-specific deadlines: • Gives licensees until ***August 1, 2021*** to develop, implement, and maintain an ISP. • Gives licensees until ***August 1, 2022*** 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: • Requires notification of the state regulator within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred. • Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Louisiana and the cybersecurity event has a reasonable likelihood of materially harming a consumer residing in Louisiana or any material part of the normal operations of the licensee). • Provides that the licensee has a continuing obligation to update and supplement notifications.	Expands exemptions in the NAIC Model Law to include those with: • Fewer than 25 employees (rather than 10). • Less than $5 million in gross annual revenue. • Less than $10 million in year-end total assets. • ISPs in accordance with GLBA, provided that a certification of compliance can be submitted, upon request. • ISPs in accordance with statutes, rules, and regulations of a jurisdiction approved by the state regulator, though an annual statement certifying compliance must be filed with the state regulator.	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.
Maine					

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
Maryland Md. Ins. Code § 4-406(b); Md. Bus. Code § 14-3504; Bulletin 19-14			Does not mirror the NAIC Model Law. Requires carriers to notify the state regulator within 45 days of determining that a breach occurred if the carrier: • Conducts an investigation required under the state's data breach notification law; and • Determines that the breach creates a likelihood that personal information has been or will be misused.		
Massachusetts					
Michigan Mich. Code Ann. §§ 553 et seq. ***Effective January 20, 2021***	Mirrors the NAIC Model Law, except sets two state-specific deadlines: • Gives licensees until ***January 20, 2022*** to develop, implement, and maintain an ISP. • 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: • Requires notification of the state regulator within 10 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred. • 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). • Imposes industry-specific requirements governing notification to consumers (e.g.,	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
			dictates appropriate forms of notice).		
Minnesota					
Mississippi Miss. Stat. §§ 83-5801 et seq.	Mirrors the NAIC Model Law, except does <u>not</u> 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: • Requires notification of the Commissioner within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred. • Establishes more specific criteria to trigger notification to the state regulator (i.e., requires notification if the licensee is licensed in Mississippi <u>and</u> 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: • Fewer than 50 employees (rather than 10). • Less than $5 million in gross annual revenue. • Less than $10 million in year-end total assets. • Producer and adjuster licenses from the ISP requirements and the investigation and notice requirements (but only to the extent they concern cybersecurity events at TPSPs). Exempts licensees affiliated with a depository institution that maintains an ISP in accordance with GLBA from the ISP requirements.	N/A
Missouri					
Montana					
Nebraska					

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
Nevada					
New Hampshire 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. 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: • Requires notification of the Commissioner within 3 business days (rather than 72 hours) of a determination that a cybersecurity event has occurred. • 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: • Licensees with fewer than 20 employees (rather than 10). • Licensees operating in compliance with New York's cybersecurity regulation. • Continuing care retirement communities. • Life settlement providers. • Licensees that are banks or credit unions and that maintain an ISP in accordance with GLBA. • Motor vehicle retail sellers/sales finance company. • "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					
New York	Requires implementation of a "Cybersecurity Program" and dictates its "core cybersecurity	N/A	Requires notification of the state regulator within 72 hours of a	Offers several exemptions (to varying sections) for:	Requires designation of a "Chief

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
23 NYCCR 500 ***Note, the New York rules pre-date the NAIC Model Law***	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.). 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. Like the NAIC Model Law, requires the Cybersecurity Program to: • Be based on a risk assessment. • 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. • Establish a written incident response plan. • Submit an annual certification to the state regulator by February 15.		determination that a cybersecurity event has occurred that is either: • 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 • A cybersecurity event that has a reasonable likelihood of materially harming any material part of the normal operations of the licensee.	• Licensees with fewer than 10 employees located in New York. • Licensees with less than $5 million in gross annual revenue in each of the last three fiscal years from New York business operations. • Licensees with less than $10 million in year-end total assets. • Employees, agents, representatives or designees of licensees. • Licensees that do not directly/indirectly operate, maintain, utilize, or control any information systems. • Licensees that do not directly/indirectly control, own, access, etc. nonpublic information. Requires licensees that qualify for exemptions to file a Notice of Exemption.	Information Security Officer" to oversee and implement the Cybersecurity Program, report annually to the licensee's board of directors, etc. Requires the licensee to utilize qualified cybersecurity personnel to manage their cybersecurity risks/oversee the core cybersecurity functions. Unlike the NAIC Model Law, provides for specific requirements concerning TPSP security policies.

State	ISP Requirements	Investigation Requirements	Notification Requirements	Exceptions	Other
	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 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. 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 cybersecurity framework" for the purposes of the state's Uniform Commercial Code.	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. 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: • Fewer than 20 employees (rather than 10). • Less than $5 million in gross annual revenue. • Less than $10 million in year-end total assets. • 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.
Oklahoma					

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

APPENDIX 1: Application of NAIC Model Law Attestation Requirements and Exceptions

* We have drafted the below survey in response to requests from Council members for supplemental information regarding qualification as a licensee; the application of the annual certification requirements (i.e., the extent they apply to entities beyond domestic insurers); and the obligations associated with eligibility for and compliance with the exception/exemption provisions (e.g., whether filings are required for all licensees).
* While each state has adopted a slightly nuanced approach, and the below survey outlines the varying approaches in greater detail, there are some general themes worth noting at the outset in response to the questions posed by Council members:
  - ***Qualification as a Licensee***. Every state appears to have adopted the NAIC Model Law's definition of a ***licensee*** (i.e., a person who is licensed, authorized to operate, registered or required to be licensed, authorized, or registered under the state insurance laws, excluding a purchasing group or a risk retention group chartered and licensed in another state and/or a licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction). Though the definition of ***person*** varies from state-to-state, in every state it includes both an individual and an entity.
  - ***Certification Requirements***. Every state requires only ***domestic insurers/insurers domiciled in the state*** to annually certify/attest that they are compliant with the ISP requirements. Few states define who qualifies as an insurer in their state's Insurance Data Security Law; as such—to the extent possible—we have included the definition of ***insurer*** used throughout the state's insurance code.
  - ***Eligibility for Exceptions***. In general, the majority of states do not specifically address—in available guidance or otherwise—whether ***all licensees*** (even those that do qualify as insurers/do not need to submit the annual certification) are required to submit a filing that they are eligible for an exception. In such states, it is likely that—to the extent a filing is required to qualify for a given exception—such a filing is required of ***all licensees***. It warrants noting, however, that most states only require an affirmative filing that a licensee qualifies for an exception if the licensee is seeking to take advantage of an exception related to compliance with ***another regulatory regime*** (e.g., HIPAA, GLBA, New York's cybersecurity regulation, etc.). If a state has issued supplemental guidance providing a different interpretation (e.g., Mississippi, New Hampshire, Ohio, and South Carolina), it is noted in the below survey.
  - ***Application of the Licensee-Designee Exception and Associated Certification Requirements***. One question specifically asked if there are circumstances under which a ***licensee that is not an insurer*** would need to file an annual certification (i.e., if an individual licensee submits qualification for an exception pointing to a business licensee's ISP, and the business licensee otherwise qualifies for an exception, would the business licensee now need to file an attestation since the individual is operating under the business licensee's ISP?). It does not appear as though any state specifically addresses this question in available guidance, but it seems unlikely that any state would affirmatively require non-insurers to file an annual certification (unless such a certification was otherwise required by an exception that is applicable to all licensees).
* Given the limited guidance available, it warrants highlighting that the vast majority of states enacted their respective Insurance Data Security Laws in 2019 and 2020. As such, available guidance is fairly limited and—in many states—the state regulator is expected/has the authority to promulgate regulations in the coming months and/or years to implement and clarify these provisions.

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
Questions	Who qualifies as a ***licensee***?	Who is required to submit an annual attestation/certification of compliance? Who qualifies as an ***insurer***?	Are licensees required to submit a filing, written statement, certification, etc. to take advantage of any of the exceptions? If an individual/entity is not required to file an annual certification, will they still be required to submit a filing describing their eligibility for an exception?	If an individual licensee submits qualification for an exception pointing to a business licensee's ISP, and the business licensee otherwise qualifies for an exception, would the business licensee now need to file a certification since the individual is operating under the business licensee's ISP?
Alabama **Effective – May 1, 2019**	Applies to ***licensees***, defined to include a person (i.e., an individual or a nongovernmental entity) authorized to operate; registered; or required to be licensed, authorized, or registered under the state insurance laws (including insurance producers and insurance companies that do not meet the size and/or revenue-related exemptions or other exemptions). Bulletin 2019-05. Does not include: • A purchasing group or a risk retention group chartered and licensed in another state.	***By February 15, 2021***, and ***unless an exception applies***, requires ***insurers*** domiciled in Alabama to submit an annual written statement by February 15 certifying that they are in compliance with the statutory requirements. Ala. Code § 27-62-4(i). While Alabama's Insurance Data Security Law does not define ***insurer***, the state's Insurance Code defines the term to include "every person engaged as indemnitor, surety, or contractor in the business of entering into contracts of insurance." Ala. Code § 27-1-2(2).	***Does not address whether a licensee that is not required to attest will still need to file an exception (if applicable).*** Given its application to licensees, to the extent a filing is required for an exception, appears that such a filing must be filed regardless of whether a certification also had to be filed. Does not appear to require: • ***Licensees*** that qualify for the size and/or revenue-related exemptions; or • ***Employees, agents, representatives, or designees of a licensee that are also licensees*** that are covered by the ISP of the other licensee to submit a certification, attestation, or written statement to take advantage of the exception. Ala. Code § 27-62-9(a)(1), (3). Deems ***licensees*** to have met the requirements of the state's Insurance Data Security Law if they have established and maintain an ISP in compliance with:	***Does not explicitly address this question in existing guidance***, but appears unlikely that an entity that does not otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
	• A licensee that is acting as an assuming insurer that is domiciled in another state or jurisdiction. Ala. Code § 27-62-3(9), (12).		• HIPAA, provided that the licensee submits a written statement certifying compliance. Ala. Code § 27-62-9(a)(2). • GLBA, provided that the licensee produces, upon request, documentation that independently validates the depository institution's adoption of an ISP (*applies to licensees affiliated with depository institutions that maintain ISPs in compliance with GLBA*). Ala. Code § 27-62-9(a)(4).	
Connecticut **Effective – October 1, 2020**	Applies to ***licensees***, defined to include a person (i.e., an individual or a nongovernmental entity) authorized to operate; registered; or required to be licensed, authorized, or registered under the state insurance laws. Does not include: • A purchasing group or a risk retention group chartered and licensed in another state. • A licensee that is acting as an assuming insurer and domiciled in another state or jurisdiction. Conn.	***By February 15, 2021***, and ***unless an exception applies***, requires ***domestic insurers and health care centers*** to submit an annual written statement by February 15 certifying that they are in compliance with the statutory requirements. Due to COVID-19, permits licensees that fail to file their annual certification by February 15, 2021 to file by April 15, 2021 without risk of sanctions. Bulletin IC-42. While Connecticut's Insurance Data Security Law does not define ***domestic insurer***, the state's Insurance Code defines the term to include "any insurer [(i.e., any person or	***Does not address whether a licensee that is not required to attest will still need to file an exception (if applicable).*** Given its application to licensees, to the extent a filing is required for an exception, appears that such a filing must be filed regardless of whether a certification was also required. Does not appear to require: • ***Licensees*** that qualify for the size-related exemptions; or • ***Employees, agents, representatives, or designees of a licensee that are also licensees*** that are covered by the ISP of the other licensee to submit a certification, attestation, or written statement to take advantage of the exception. Conn. Gen. Stat. § 38a-38(c)(10)(A)(i), (iii). Deems ***licensees*** to have met the requirements of the state's Insurance Data Security Law if they have established and maintain an ISP in compliance with:	***Does not explicitly address this question in existing guidance***, but appears unlikely that an entity that does not otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions). But affirmatively requires licensees taking advantage of the exception applicable to those operating in compliance with other state laws to annually certify compliance.

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
	Gen. Stat. § 38a-38(b)(7), (10).	combination of persons doing any kind/form of insurance business other than a fraternal benefit society and includes a receiver of any insurer when the context reasonably permits)] that has been chartered by, incorporated, organized, or constituted within or under the laws of [Connecticut]." Conn. Gen. Stat. § 38a-1(6), (12).	• A jurisdiction approved by the Commissioner (pursuant to regulations to be adopted by the Connecticut Insurance Department), provided that the licensee submits an annual written statement certifying compliance. Conn. Gen. Stat. § 38a-38(c)(10)(A)(iv). • HIPAA, provided that the licensee submits a written statement certifying compliance. Conn. Gen. Stat. § 38a-38(c)(10)(A)(ii).	Conn. Gen. Stat. § 38a-38(c)(10)(A)(iv).
Delaware **Effective – July 1, 2019**	Applies to ***licensees***, defined to include a person (i.e., an individual, corporation, company, etc.) who is licensed, authorized to operate, registered or required to be licensed, authorized, or registered under the state insurance laws. Does not include: • A purchasing group or a risk retention group chartered and licensed in another state. • A licensee that is acting as an assuming insurer and domiciled in	***Unless an exception applies***, requires ***insurers*** domiciled in Delaware to submit an annual written statement by February 15 certifying that they are in compliance with the statutory requirements. Del. Code tit. 18, § 8604(i). Defines ***insurer*** to include an insurer, health service corporation, managed care organization, or HMO licensed under the state's Insurance Code. Del. Code tit. 18, § 8603(9).	***Does not address whether a licensee that is not required to attest will still need to file an exception (if applicable).*** Given its application to licensees, to the extent a filing is required for an exception, appears that such a filing must be filed regardless of whether a certification also had to be filed. Does not appear to require: • ***Licensees*** that qualify for the size-related exemptions; or • ***Employees, agents, representatives, or designees of a licensee that are also licensees*** that are covered by the ISP of the other licensee to submit a certification, attestation, or written statement to take advantage of the exception. Del. Code tit. 18, § 8609(a)(1), (3). Deems ***licensees*** to have met the requirements of the state's Insurance Data Security Law if they have established and maintain an ISP in	***Does not explicitly address this question in existing guidance***, but appears unlikely that an entity that does not otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
	another state or jurisdiction. Del. Code tit. 18, §§ 102(11), 8603(10), (14); UA Bulletin No. 5.		compliance with HIPAA, provided that the licensee submits a written statement certifying compliance. Del. Code tit. 18, § 8609(a)(2).	
Indiana **Effective – July 1, 2020**	Applies to ***licensees***, defined to include a person (i.e., individuals, corporations, associations, etc.) who is licensed, authorized to operate, registered or required to be licensed, authorized, or registered under the state insurance laws. Does not include: • A purchasing group or a risk retention group chartered and licensed in another state. • A licensee that is acting as an assuming insurer and domiciled in another state or jurisdiction. Ind. Code §§ 27-2-27-10; 27-1-2-3(h).	***Unless an exception applies***, requires ***insurers*** domiciled in Indiana to submit an annual written statement by April 15 certifying that they are in compliance with the requirements associated with developing an ISP, conducting a risk assessment, etc. Ind. Code § 27-2-27-20(c). While Indiana's Insurance Data Security Law does not define ***insurer***, the state's Insurance Code defines the term to include "a company, firm, partnership, association, order, society or system making any kind of insurance," including associations operating as Lloyds, reciprocal or inter-insurers, or individual underwriters. Ind. Code § 27-1-2-3(x).	***Does not address whether a licensee that is not required to attest will still need to file an exception***, but does not appear to require: • ***Licensees*** that qualify for the size and/or revenue-related exemptions; • ***Licensees*** that have established and maintain ISPs under HIPAA; • ***Employees, agents, representatives, or designees of a licensee that are also licensees*** that are covered by the ISP of the other licensee; or • ***Licensees affiliated with financial institutions*** that maintain an ISP in compliance with GLBA to submit a certification, attestation, or written statement to take advantage of the exception. Ind. Code § 27-2-27-26.	***Does not explicitly address this question in existing guidance***, but appears unlikely that an entity that does not otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
Louisiana **Effective – August 1, 2021**	Applies to ***licensees***, defined to include a person (i.e., any natural person or nongovernmental juridical person) who is licensed, authorized to operate, registered or required to be licensed, authorized, or registered under the state insurance laws. Cybersecurity Guidance. Does not include: • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. La. Rev. Stat. § 22:2503(7), (10).	***By February 15, 2022***, and ***unless an exception applies***, requires ***insurers*** domiciled in Louisiana to submit an annual written statement by February 15 certifying that they are in compliance with the ISP requirements. La. Rev. Stat. § 22:2504(I)(1). While Louisiana's Insurance Data Security Law does not define ***insurer***, the state's Insurance Code defines the term to include "every person engaged in the business of making contracts of insurance, other than a fraternal benefit society," including a reciprocal, insurance exchange, insurance exchange syndicate, a Lloyds organization, HMOs (for specific purposes), etc. La. Rev. Stat. § 22:46(10).	***Does not address whether a licensee that is not required to attest will still need to file an exception (if applicable).*** Given its application to licensees, to the extent a filing is required for an exception, appears that such a filing must be filed regardless of whether a certification also had to be filed. Does not appear to require: • ***Licensees*** that qualify for the size and/or revenue-related exemptions; or • ***Employees, agents, representatives, or designees of a licensee that are also licensees*** that are covered by the ISP of the other licensee to submit a certification, attestation, or written statement to take advantage of the exception. La. Rev. Stat. § 22:2509(A)(1)-(3), (5). Deems ***licensees*** to have met the requirements of the state's Insurance Data Security Law if they have established and maintain an ISP in compliance with: • HIPAA, provided that the licensee submits, upon request, a written statement certifying compliance. La. Rev. Stat. § 22:2509(A)(4). • GLBA, provided that the licensee produces, upon request, documentation that independently validates the depository institution's adoption of an ISP (*applies to licensees affiliated with depository institutions that maintain ISPs in compliance with GLBA*). La. Rev. Stat. § 22:2509(A)(6).	***Does not explicitly address this question in existing guidance***, but appears unlikely that an entity that does not otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
			• A jurisdiction approved by the Commissioner, provided that the licensee submits a written statement certifying compliance. La. Rev. Stat. § 22:2509(A)(7).	
Michigan **Effective – January 20, 2021**	Applies to ***licensees***, defined to include a licensed insurer, producer, and other persons licensed, authorized, or registered or holding or required to hold a certificate of authority under the state's insurance laws. Does not include: • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. Mich. Comp. L. Ann. § 500.553(g).	***By February 15, 2022***, and ***unless an exception applies***, requires ***insurers*** domiciled in Michigan to submit an annual written statement by February 15 certifying that they are in compliance with the ISP requirements. Mich. Comp. L. Ann. § 500.555(9). While Michigan's Insurance Data Security Law does not define ***insurer***, the state's Insurance Code defines the term to include an individual, corporation, inter-insurer, Lloyds organization, etc., engaged/attempting to engage in the business of making insurance or surety contracts. Mich. Comp. L. Ann. § 500.106.	***Does not address whether a licensee that is not required to attest will still need to file an exception (if applicable).*** Given its application to licensees, to the extent a filing is required for an exception, appears that such a filing must be filed regardless of whether a certification also had to be filed. Does not appear to require: • ***Licensees*** that qualify for the size-related exemptions; • ***Employees, agents, representatives, or designees of a licensee that are also licensees*** that are covered by the ISP of another licensee; or • ***Licensees*** that have established and maintain an ISP in compliance with HIPAA. to submit a certification, attestation, or written statement to take advantage of the exception. Mich. Comp. L. Ann. § 500.565(1)-(3).	***Does not explicitly address this question in existing guidance***, but appears unlikely that an entity that does not otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).
Mississippi	Applies to ***licensees***, defined to include a person (i.e., any natural	***Unless an exception applies***, requires ***insurers*** domiciled in Mississippi to	***Per guidance from the Mississippi Insurance Department, only requires licensees who are insurers and have an NAIC # to complete the***	***Does not explicitly address this question in existing guidance***, but

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
Effective – July 1, 2019	person or nongovernmental juridical person) who is licensed, authorized to operate, registered or required to be licensed, authorized, or registered under the state insurance laws. Does not include: • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. Miss. Code Ann. § 83-5-805.	submit an annual written statement by February 15 certifying that they are in compliance with the ISP requirements. Miss. Code Ann. § 83-5-807(9); Bulletin 2019-4; Mississippi Cybersecurity Law Guidance; Mississippi Insurance Data Security Law ISP Certification Form. While Mississippi's Insurance Data Security Law does not define ***insurer***, the state's Insurance Code defines the term to include "those companies subject to the jurisdiction of the commissioner" (i.e., all indemnity or guaranty companies, all companies, corporations, etc. transacting the business of insurance in this state). Miss. Code Ann. §§ 83-5-1, 83-6-1(e).	***exception certification form***. Mississippi Cybersecurity Law Guidance. Generally, does not appear to require: • ***Licensees*** that qualify for the size and/or revenue-related exemptions; • ***Employees, agents, representatives, or designees of a licensee that are also licensees*** that are covered by the ISP of the other licensee; or • ***Insurance producers and adjusters*** to—among other things—submit a certification, attestation, or written statement to take advantage of the exception. Miss. Code Ann. § 83-5-817(a), (c). But indicates via guidance that ***licensees who are insurers and have an NAIC #*** are required to complete an exception certification form, even for these exceptions. Mississippi Cybersecurity Law Guidance. Deems ***licensees*** to have met the requirements of the state's Insurance Data Security Law if they have established and maintain an ISP in compliance with: • HIPAA, provided that the licensee submits a written statement certifying compliance. Miss. Code Ann. § 83-5-817(b). • GLBA, provided that the licensee produces, upon request, documentation that independently validates the depository institution's adoption of an ISP (*applies to licensees affiliated with depository institutions that maintain ISPs in compliance with GLBA*). Miss. Code Ann. § 83-5-817(d).	appears unlikely that an entity that does not otherwise qualify as an insurer would need to comply with the annual certification requirements. Mississippi Insurance Data Security Law ISP Certification Form.

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
New Hampshire **Effective – January 1, 2020**	Applies to ***licensees***, defined to include a person (i.e., an individual or non-governmental entity) who is licensed, authorized to operate, registered or required to be licensed, authorized, or registered under the state insurance laws. Does not include: • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. N.H. Rev. Stat. § 420-P:3(IX), (XII).	***Per guidance from the New Hampshire Insurance Department, does not require licensees—other than domestic insurers—to submit the annual attestations or otherwise certify compliance with the ISP requirements*** (unless required by an exception/safe harbor)**.** Docket No. INS 20-013-AB. ***Unless an exception/safe harbor applies***, requires ***insurers*** domiciled in Mississippi to submit an annual written statement by March 1 certifying that they are in compliance with the ISP requirements. N.H. Rev. Stat. § 420-P:4(IX); Docket No. INS 20-013-AB; Bulletin INS-20-001-AB; New Hampshire Insurance Data Security Law ISP Certification Form (indicates application to domestic insurers).	***Per guidance from the New Hampshire Insurance Department, outlines circumstances in which other licensees (i.e., entities that are not insurers/not required to file an annual attestation) will be required to complete an exception certification form.*** To the extent a licensee qualifies for a safe harbor (i.e., compliance with HIPAA or New York cybersecurity regulations), requires licensees that are not domestic insurers to submit the exception certification form ***only once*** by March 1, 2021. Docket No. INS 20-013-AB; New Hampshire Insurance Data Security Law Exception Certification Form. For insurers who qualify for a safe harbor (i.e., are compliant with HIPAA or New York cybersecurity regulations), permits submission of the exception certification form in place of the ISP certification form annually by March 1. Docket No. INS 20-013-AB; New Hampshire Insurance Data Security Law Exception Certification Form. In general, does not appear to require: • ***Licensees*** that qualify for the size-related exemptions; • ***Employees, agents, representatives, or designees of a licensee that are also licensees*** that are covered by the ISP of the other licensee; or • ***Continuing care retirement communities***; • ***Life settlement providers***; • ***Licensees*** that are bank or credit unions that are compliant with GLBA;	***Does not explicitly address this question in existing guidance***, but appears unlikely that an entity that does not otherwise qualify as an insurer would need to comply with the annual certification requirements under any circumstances (e.g., the exception certification form is only required to be filed by all other licensees ***once*** by ***March 1, 2021***; domestic insurers are the only entities required to certify compliance with the ISP requirements either via an annual certification or the exception certification). Docket No. INS 20-013-AB.

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
			• ***Motor vehicle retail sellers or motor vehicle sales finance companies***; or • ***A portable electronics vendor*** to submit a certification, attestation, or written statement to take advantage of the exception. N.H. Rev. Stat. § 420-P:9 (exceptions). Deems ***licensees*** to have met the requirements of the state's Insurance Data Security Law if they have established and maintain an ISP in compliance with: • HIPAA, provided that the licensee submits a written statement certifying compliance (*extends protections to the extent that a licensee maintains other nonpublic information in the same manner as PHI, provided that the licensee submits a written statement that it does maintain and protect other nonpublic information as it does PHI*). N.H. Rev. Stat. § 420-P:10 (safe harbor). • New York's cybersecurity regulations, provided that the licensee submits a written statement certifying compliance. N.H. Rev. Stat. § 420-P:11 (safe harbor).	
Ohio **Effective – March 20, 2019**	Applies to ***licensees***, defined to include a person (i.e., an individual or business entity) who is licensed, authorized to operate, registered or required to be licensed, authorized, or registered under the state insurance laws.	***Per guidance from the Ohio Department of Insurance, only requires domestic insurers to file an ISP certification statement or indicate which exemption they meet.*** FAQs. ***Unless an exemption applies***, requires ***insurers***	***Per guidance from the Ohio Department of Insurance, only requires domestic insurers to certify the existence of an ISP or file a notice of exemption.*** ISP Certification Notice of Exemption. In general, does not appear to require: • ***Licensees*** that qualify for the size and/or revenue-related exemptions; or	***Does not explicitly address this question in existing guidance***, but appears unlikely that an entity that does not otherwise qualify as an insurer would need to comply with the annual certification requirements (e.g., domestic insurers

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
	Does not include: • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. Ohio Rev. Code § 3965.01(M).	domiciled in Ohio to submit an annual written statement by February 15 certifying that they are in compliance with the ISP requirements. Ohio Rev. Code § 3965.02(I)(1). Offers limited circumstances under which a domestic insurer may file annually on June 1. Ohio Rev. Code § 3965.02(I)(2); FAQs; ISP Certification Notice of Exemption. Defines ***insurer*** to include "any person engaged in the business of insurance, guaranty, or membership; an inter-insurance exchange; a mutual or fraternal benefit society; or a health insuring corporation. Ohio Rev. Code § 3901.32(F). ***Additional information on methods and deadlines for certifying to the presence of an ISP is forthcoming.*** Statement of Compliance with HIPAA Privacy & Security Rules Guidance Document.	• ***Employees, agents, representatives, or designees of a licensee that are also licensees*** that are covered by the ISP of the other licensee to submit a certification, attestation, or written statement to take advantage of the exemption. Ohio Rev. Code § 3965.07(A), (C). Deems ***licensees*** to have met the requirements of the state's Insurance Data Security Law if they have established and maintain an ISP in compliance with HIPAA's privacy and security rules, provided that the licensee submits a written statement certifying compliance. Ohio Rev. Code § 3965.07(B); HIPAA Compliance Certification Statement. ***Note, per guidance from the Ohio Department of Insurance, this certification statement is only required of domestic insurers.*** ODI ISP Certification Notice of Exemption. ***Additional information on the remaining exemption statuses and their application is forthcoming.*** Statement of Compliance with HIPAA Privacy & Security Rules Guidance Document.	are the only entities required to file an ISP certification statement or notice of exemption). FAQs.
South Carolina	Applies to ***licensees***, defined to include a person (i.e., an individual or business entity) who is	***Unless an exception applies***, requires ***insurers*** domiciled in South Carolina to submit an annual written	***Per guidance from the South Carolina Department of Insurance, does not require licensees to proactively communicate their exemption status, though the Department***	***Does not explicitly address this question in existing guidance***, but appears unlikely that an

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
Effective – January 1, 2019	licensed, authorized to operate, registered or required to be licensed, authorized, or registered under the state insurance laws. Bulletin No. 2018-02. Does not include: • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. S.C. Code § 38-99-10(9).	statement by February 15 certifying that they are in compliance with the ISP requirements. S.C. Code § 38-99-20(I). Clarifies that such domestic insurers will be contacted directly by the Financial Regulation & Solvency Division with further instructions. SCDOI Cybersecurity Portal. While South Carolina's Insurance Data Security Law does not define ***insurer***, the state's Insurance Code defines the term to include a corporation, fraternal organization, individual, etc. engaging/attempting to engage as principals in any kind of insurance or surety business. *See* S.C. Code § 38-1-20(33).	***may conduct random inspections to determine compliance.*** Bulletin No. 2018-12. Separately, suggests that—to take advantage of the exemptions applicable to entities compliant with HIPAA or the New York cybersecurity regulations—annual certification is required. SCDOI Presentation on Complying with the South Carolina Insurance Data Security Act. Given its application to licensees, to the extent a filing is required for an exception, appears that such a filing must be filed regardless of whether a certification also had to be filed. In general, does not appear to require: • ***Licensees*** that qualify for the size-related exemption; or • ***Employees, agents, representatives, or designees of a licensee that are also licensees*** that are covered by the ISP of the other licensee to submit a certification, attestation, or written statement to take advantage of the exception. S.C. Code § 38-1-70(A)(1)-(2). Deems ***licensees*** to have met the requirements of the state's Insurance Data Security Law if they have established and maintain an ISP in compliance with: • HIPAA, provided that the licensee submits a written statement certifying compliance. S.C. Code § 38-1-70(A)(3). • New York's cybersecurity regulation, provided that the licensee submits a written statement certifying its compliance. Bulletin No. 2018-12.	entity that does not otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).

States	Application	Annual Certification	Exceptions	Exception/Attestation Interaction
Virginia **Effective – July 1, 2020**	Applies to ***licensees***, defined to include a person (i.e., an individual or business entity) who is licensed, authorized to operate, registered or required to be licensed, authorized, or registered under the state insurance laws. Does not include: • A purchasing group or a risk retention group chartered and licensed in another state. • A person that is acting as an assuming insurer and domiciled in another state or jurisdiction. Va. Code Ann. § 38.2-621.	***Beginning in 2023***, and ***unless an exception applies***, requires ***insurers*** domiciled in Virginia to submit an annual written statement by February 15 certifying that they are in compliance with the ISP requirements. Va. Code Ann. § 38.2-623(H). Clarifies that such domestic insurers will be contacted directly by the Financial Regulation & Solvency Division with further instructions. SCC Cybersecurity Portal. While Virginia's Insurance Data Security Law does not define ***insurer***, the state's Insurance Code defines the term to include "any company engaged in the business of making contracts of insurance." Va. Code Ann. § 38.2-100.	***Does not address whether a licensee that is not required to attest will still need to file an exception (if applicable).*** Given its application to licensees, to the extent a filing is required for an exception, appears that such a filing must be filed regardless of whether a certification also had to be filed. Does not appear to require ***employees, agents, representatives, or designees of a licensee that are also licensees*** that are covered by the ISP of the other licensee to submit a certification, attestation, or written statement to take advantage of the exception. Va. Code Ann. § 38.2-629(A)(2). Deems ***licensees*** to have met the requirements of the state's Insurance Data Security Law if they have established and maintain an ISP in compliance with: • HIPAA, provided that the licensee submits a written statement certifying compliance. Va. Code Ann. § 38.2-629(A)(1). • GLBA, provided that the licensee produces, upon request, documentation that independently validates the depository institution's adoption of an ISP (*applies to licensees affiliated with depository institutions that maintain ISPs in compliance with GLBA*). Va. Code Ann. § 38.2-629(A)(3).	***Does not explicitly address this question in existing guidance***, but appears unlikely that an entity that does not otherwise qualify as an insurer would need to comply with the annual certification requirements (i.e., the statute provides that if an exception applies, the licensee will be exempt from—among other things—the certification provisions).