COMMONWEALTH OF VIRGINIA

STATE CORPORATION COMMISSION

COMMONWEALTH OF VIRGINIA, *ex rel.*

STATE CORPORATION COMMISSION

CASE NO. INS-2020-00168

Ex Parte: In the matter of Adopting
Rules to Implement the Requirements
of the Insurance Data Security Act

THE BUREAU OF INSURANCE'S RESPONSE TO COMMENTS

I. Introduction

On August 13, 2020, the State Corporation Commission ("Commission") issued an Order to Take Notice introducing proposed regulations drafted by its Bureau of Insurance ("Bureau") to adopt new rules at Title 14, Chapter 430 of the Virginia Administrative Code (14VAC5-430-10 *et seq.*), entitled Insurance Data Security Risk Assessment and Reporting ("Rules"), and seeking comments to the Rules on or before October 26, 2020.[1]

The Bureau drafted and proposed the Rules to comply with the requirements of the Insurance Data Security Act, §§ 38.2-621 *et seq.* of the Code of Virginia ("IDSA"). The IDSA was enacted by the 2020 Virginia General Assembly and establishes standards that Bureau licensees must meet regarding data security, cybersecurity investigations, and notification to the

[1] Comments to the Rules were filed with the Clerk o the Commission ("Clerk") by **Wesley Bissett**, Independent Agents and Brokers of America ("IIABA"); **Robert Bradshaw**, on behalf of Independent Insurance Agents of Virginia ("IIAV"), as well as on behalf of Christine E. Miller, ("NAIFA"), Kevin Kowar, Professional Insurance Agents of Virginia/DC ("PIA"), Kathie Naylor, Virginia Association of Health Underwriters ("VAHU"); **Nancy Egan**, American Property Casualty Insurance Association ("APCIA"); **Marc Follmer**, Virginia Farm Bureau Mutual Insurance Company ("VFB"); **Michelle Caroll Foster**, American Council of Life Insurers ("ACLI"); **Leigh Hubbard**, Virginia Land Title Association ("VLTA"); **Andrew Kirkner**, National Association of Mutual Insurance Companies ("NAMIC"); and **John Morris**, UnitedHealthcare ("UHC"). Comments submitted by NAIMIC, IIABA and UHC were filed with the Clerk on October 27, 2020, after the deadline imposed by the Order to Take Notice. However, the Bureau has considered and addressed all comments filed regardless of when such comments were filed.

Commissioner of Insurance ("Commissioner") and consumers of cybersecurity events. The IDSA also directs the Commission to adopt regulations to implement the requirements of the IDSA.[2]

Though modeled on the National Association of Insurance Commissioners' ("NAIC") Insurance Data Security Model Law ("NAIC Model Law"), the Virginia General Assembly did not adopt the NAIC Model Law verbatim and instead revised the model rules as it deemed appropriate. Thus, when drafting its proposed Rules, the Bureau deferred to the requirements outlined by the IDSA if there was any conflict between the NAIC Model Law and the IDSA.

As outlined below, in response to the comments, the Bureau has either proposed certain changes to the Rules or identified why the Bureau believes certain proposed revisions cannot or should not be made. A copy of the revisions to the Rules as proposed by the Bureau are attached as Attachment A ("Revised Rules").

II. The Bureau's Proposed Revisions In Response to Certain Comments

A. 14 VAC 5-430-30. *Definition of "Level One Licensee" and "Level Two Licensee"*

The Rules originally included definitions for a "level one licensee" (*i.e.* a licensee having more than 10 authorized persons with access to certain consumer data) and a "level two licensee" (a licensee having 10 or fewer authorized persons with access to certain consumer data). The Bureau differentiated when and how each category of licensee was required to assess and develop an information security program, in an attempt to reduce the burden on smaller licensees and prevent inconsistent regulatory requirements for larger licensees.

However, several of the commenters objected to this bifurcated approach and the regulatory implications of this distinction, asserting that varying the compliance requirements for

[2] *See* § 38.2-627 D of the IDSA.

different types of licensees was confusing, unfair, and cumbersome to monitor- especially for those licensees hovering around 10 authorized persons.[3] Additionally, several commenters sought clarification as to who (*i.e.* employees, third party contractors, etc.) should be counted as an "authorized person" when determining whether a licensee was a level one or level two. Other commenters asked for clarification about how the National Institute of Standards and Technology ("NIST") cybersecurity referenced in the Rules would be applied to the two types of licensees. Overall, most of the commenters recommended significant modification to, or complete removal of, the "level one licensee" versus "level two licensee" distinction.

In response to these comments, the Bureau decided to abandon the bifurcated approach and remove the distinction between level one and level two licensees. In the Revised Rules, the Bureau has eliminated the definition of each of these licensee types, and has removed any compliance distinction between licensee types, including in 14 VAC 5-430-30, 14 VAC 5-430-40 and 14 VAC 5-430-50. Instead, the Revised Proposed Rules still require licensees to develop information security programs as required by IDSA, but allow these programs to be tailored as appropriate to the size and complexity of the particular licensee and the type of information it possesses, instead of based upon a bright-line "level" categorization. Licensees may use the minimum program standards, as identified in the IDSA, or the applicable NIST standards (or any other substantially similar standards) as a basis for developing an appropriate program.

[3] *See e.g.* Bradshaw Comments, ACLI Comments at 1-2, VLTA Comments at 2-3, IIABA Comments at 2, and NAMIC Comments at 1-2.

B. 14 VAC 5-430-30. Definition of "Publicly Available Information"

VLTA requested that a definition of the term "publicly available information" be added, as this term is used within the definition of "nonpublic information."[4] The Bureau has added this definition as identified in the attached Revised Rules.

C. 14 VAC 5-430-50 (B)(6). Multi-factor authentication

14 VAC 5-430-50 (B)(6) allows licensees to use a variety of authentication factors ("multi-factor authentication") when implementing a cybersecurity program. APCIA was concerned that this provision required licensees to adopt prescribed security measures instead of allowing licensees the flexibility to adopt risk-based security measures appropriate to a particular situation.[5] Accordingly, APCIA requested that this provision be amended to provide that licensees "[i]mplement effective controls, which may ~~including~~ include multi-factor authentication" for authorized access to nonpublic information.[6] The Bureau is amenable to this revision and has included it in 14 VAC 5-430-50(B)(6) in the attached Revised Rules.

D. 14 VAC 5-430-60. Reporting Cybersecurity Events to the Commissioner

Several of the commenters raised concerns regarding reporting cybersecurity events to the Commissioner. Specifically, ACLI, APCIA and NAMIC asserted that 14 VAC 5-430-60 (A)(3)'s requirement that licensees continue to update the Commissioner about the status of a cybersecurity event "until the licensee has provided all information set out in § 38.2-625 of the [IDSA]" was unrealistic and overburdensome, because § 38.2-625 of the IDSA contained a

[4] VLTA Comments at 1.

[5] APCIA Comments at 2.

[6] *Id.*

lengthy list of information that the licensee may never actually have access to or possess.[7] One of these commenters noted that the General Assembly addressed this concern by requiring licensees to report only "as much of the information as possible" to the Commissioner, acknowledging that not all of the identified information may ultimately be known or uncovered.[8] Accordingly, the Bureau proposes amending the proposed Rules by also adding the phrase "as much of this information [. . .] as possible," in paragraph A.3. of 14 VAC 5-430-60 to maintain consistency with the IDSA and clarify reporting obligations to the Commissioner.

In addition, a NAMIC member asked the Bureau to revise 14 VAC 5-430-60 to clarify that a licensee was required to report a cybersecurity event to the Commissioner only when the licensee has determined *both* that a cybersecurity event has occurred *and* there is a duty to report it.[9] Though the Bureau believes this was the original intent of the Rules as presented, it has incorporated the proposed clarification into 14 VAC 5-430-60 as requested.

E. 14 VAC 5-430-70. HIPAA Exemption

UHC submitted several comments seeking clarification regarding a licensee's compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") as a way to comply with the Rules and the IDSA.[10] Specifically, UHC asked for confirmation that a HIPAA compliant licensee who already meets the requirements in §38.2-629(A)(l) of the IDSA would be considered compliant with (a) IDSA's requirements for establishing an information security

[7] *See e.g.* ACLI Comments at 3, APCIA Comments at 2, and NAMIC Comments at 4.

[8] *See e.g., id.*

[9] *See* NAMIC Comments at 4.

[10] *See* UHC Comments at 1.

program,[11] and the requirements contained in these Rules; (b) IDSA's requirements regarding the investigation of a cybersecurity event[12] and the requirements of 14 VAC 5-430-50 of this Rule; and,.(c) IDSA's requirements regarding notice to consumers[13] and the requirements contained in 14 VAC 5-430-70 of this Rule.

Because HIPAA compliant licensees must already meet or exceed cybersecurity requirements contained in the IDSA,[14] the Bureau presumes that § 38.2-629 of the IDSA intended to excuse HIPAA-compliant licensees from any requirement to implement a separate risk assessment plan, information security programs or cybersecurity event investigative process. However, the Bureau proposes amending the first sentence in 14 VAC 5-430-70 A of the Rules to read "[l]icensees, *except those exempt under subsections A 1 and A 2 § 38.2-629 of the Code of Virginia* . . ." to clarify the Bureau's position that HIPPA compliant licensees are excused from these IDSA requirements and address UHC's concerns.

III. Certain Proposed Revisions Cannot be Adopted Because of Statutory Limitations

A. Request to Abandon the Rules Completely

IIABA proffered that the Rules were not necessary and urged the Bureau to reconsider implementing the Rules at all.[15] However, § 38.2-627 of the IDSA provides that "[t]he Commission shall adopt rules and regulations implementing the provisions of" the IDSA. As

[11] *See* § 38.2-623 of the ISDA.

[12] *See* § 38.2-624 of the ISDA.

[13] *See* § 38.2-624 of the ISDA.

[14] HIPPA's data security requirements are substantially similar to those contained in NIST. *See* Special Publication 800-66. https://csrc.nist.gov/publications/detail/sp/800-66/rev-1/final

[15] IIABA Comments at 1.

such, the Bureau believes that the implementation of these Rules is required and declines to recommend that the Commission abandon this rulemaking process.

B. Reciprocal Compliance with Other States' Laws

IIAV, NAMIC and VLTA asked that the Rules be revised to reflect that licensees who were already complying with cybersecurity standards enacted by other states be exempt from complying with the IDSA and the Rules or be provided a "safe harbor" for compliance with another state's cybersecurity requirements.[16] These commenters argue because the NAIC Model Law's drafters intended that such exemptions or safe harbors be allowed, and Virginia's General Assembly relied (at least in part) upon NAIC's Model Law when enacting the IDSA, such exemptions should be allowed.[17]

However, the IDSA neither provides for such exemptions, nor allows the Bureau to create its own exemptions. Moreover, hinging compliance upon other states' laws and regulations limits the Bureau's ability to regulate licensees as it deems appropriate to comply with the IDSA and protect Virginia consumers. Accordingly, the Bureau declines recommending that the Commission adopt these requested revisions.

C. Requested small licensee exemption

Certain commenters also requested that the Bureau consider including a small business exemption, similar to that adopted by NAIC's Model Law, thus eliminating the requirement for

[16] *See e.g.*, Bradshaw Comments at 1, NAMIC Comments at 4-5, and VLTA Comments at 2.

[17] The Bureau notes, however, that the NAIC Model Law does *not* include an express exemption for licensees complying with other state's laws, but instead, includes only a drafting note that licensees compliant with the New York's *Cybersecurity Requirements for Financial Services Companies*, were compliant with the NAIC Model Law at that time.

certain small businesses to meet any of the IDSA's requirements.[18] However, the General Assembly did not adopt a small business exemption in the IDSA, nor authorized the Bureau to create its own exemptions.[19] Accordingly, the Bureau declines recommending that the Commission adopt these requested revisions.

IV. Other of the Proposed Revisions Are Either Not Warranted or Necessary

A. 14 VAC 5-430-30. Definition of "multi-factor authentication"

VFB requested that the Bureau specifically reference "Device-Based Digital Certificates" within the definition of multi-factor authentication, as an example of an authorized multi-factor authentication.[20] However, the Bureau has opted to retain the general term "multi-factor authentication" without further limitation in the Revised Rules. The Bureau's identified definition of "multi-factor authentication" is universally accepted in the industry[21] and encompasses *all* multi-factor authentication factors, including, *but not limited to,* the use of a device-based digital certificate.[22] Further defining this term with only a few enumerated illustrative methods could signal that other methods not specifically listed in the definition would not be allowed. This is not the Bureau's intent and would contradict industry standards. As such, the Bureau declines recommending that the Commission adopt this proposed revision.

---

[18] *See e.g.* Bradshaw Comments, and IIABA Comments.

[19] *See e.g.* § 38.2-627 of the IDSA. Additionally, if small businesses were exempted from IDSA, it would default to regulation by federal authorities pursuant to the Graham Leach Bliley Act, 15 U.S.C. § 6801 *et seq.*, creating a potential inconsistency in the regulation of Bureau's licensees and how each was required to prevent, manage and report cybersecurity events.

[20] VFB Comments at 1.

[21] *See* https://csrc.nist.gov/glossary/term/Multi_Factor_Authentication and https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2018/the-multiple-options-for-multi-factor-authentication.

[22] *See* https://www.networkworld.com/article/2350520/achieving-two-factor-authentication

A. 14VAC5-430-40 A 4. Proposed Elimination of Certain Language

VLTA requested that the phrase "*implement information safeguards to manage the threats identified in the licensee's ongoing assessment*" be removed from the proposed regulation, asserting that 14VAC5-430-*40* was only intended to address the cybersecurity *assessment* process, and that only 14 VAC 5-430-*50* should address *implementation* of cybersecurity safeguards.[23] The Bureau disagrees; 14 VAC 5-430-40 includes implementation of safeguards as an important part of the overall assessment process, while 14 VAC 5-430-50 outlines in detail how implementation of these safeguards should be conducted. Thus, contrary to VLTA's position, no inconsistency is created by referencing program implementation in 14 VAC 5-430-40. As such the Bureau declines recommending that the Commission adopt VLTA's proposed revision.

C. 14VAC5-430-60. Trigger for Notice

VFB commented that the Bureau had not established what number of consumers must be harmed to trigger notice to the Commissioner of a cybersecurity event.[24] However, the Bureau in fact did set a threshold for reporting and stated that *any* number of consumers harmed would trigger the reporting requirement outlined by 14 VAC 5-430-60. The Bureau believes this single consumer reporting threshold is reasonable because the Bureau is as concerned about any occurrence of a cybersecurity event, as it is the number of consumers impacted. As such, the Bureau does not believe any revision to the Revised Rules in this regard was necessary.

---

[23] *See* VLTA Comments at 1-2.

[24] VFB Comments at 2.

D. 14 VAC 5-430-60. Reporting Process

APCIA asked that the Bureau revise its proposed two-step reporting process requiring licensees to initially report an incident to the Bureau via email, and then receive further instruction for submission of confidential information through a secure portal system.[25] APCIA instead asked that the Bureau consider allowing reporting through *either* of these means.

As outlined in the Rules, after receiving an email alert from a licensee that a cybersecurity event has occurred (which presumably would not include non-public information), the Bureau will then create a separate and secure portal which the licensee can use to submit information (both public and non-public) relating to that event. The portal will be segregated and secured for use only by the Bureau and that particular licensee for that particular event, to avoid inadvertent access by others and ensure the integrity of the information submitted. Email platforms alone do not provide the security necessary to manage receipt of confidential information, and an appropriately tailored portal cannot be created until an event is reported or known. Thus, the Bureau believes its two-step process implements best practices for managing the cybersecurity event reporting process and declines recommending that the Commission adopt the requested revision.

E. 14 VAC 5-430-70 B and C. Notice to the Commissioner of Licensee's Decision to Withhold Notice to Consumers

The Rules originally provided that if a licensee determined a cybersecurity event did not rise to a level requiring consumer notification, that it provide a detailed explanation of this decision to the Commissioner. The Commissioner then had the ability to review and override that decision, requiring licensees to provide notice of a cybersecurity event to consumers. ACLI,

[25] APCIA Comments at 2.

APCIA and NAMIC requested that these "override provisions" be eliminated completely, or instead that the Bureau simply require licensees to maintain documentation of the determination not to send notice for a set period of time.[26]

In the Revised Proposed Rules, the Bureau has agreed to delete subsection 14 VAC 5-430-70 C which allows the Commissioner to reverse a licensee's decision not to report a cybersecurity event to consumers. However, the Bureau still wants to know when a licensee decides not to inform consumers of a cybersecurity event and the bases for that decision, which will allow for further discussion of the matter.[27]

V. Conclusion

Accordingly, for the reasons cited above, the Bureau respectfully requests that the Commission enter an order adopting the Revised Rules as attached without any need for additional comments or hearing[28]on these matters.

[26] *See e.g.* ACLI Comments at 3, APCIA Comments at 2-3, and NAMIC Comments at 4.

[27] Additionally, § 38.2-624 of the IDSA includes a five-year record retention requirement, which would also require that records relating to a decision not to report an event to consumers be maintained for five years as well.

[28]Additionally, the Bureau clarified with the one commenter who alluded to the possibility of a hearing- Mr. Bradshaw- that he was not requesting a hearing at this time.

Respectfully submitted,

BUREAU OF INSURANCE OF THE
STATE CORPORATION COMMISSION

By: */s/ Patricia A.C. McCullagh*
Patricia A.C. McCullagh
Deputy Chief Counsel-Financial Services

Patricia A. C. McCullagh, Deputy Chief Counsel
Office of General Counsel
State Corporation Commission
P.O. Box 1197
Richmond, Virginia 23218
(804) 371-9671
(804) 371-9240
Patricia.McCullagh@scc.virginia.gov

Dated: April 5, 2021

CERTIFICATE OF SERVICE

I hereby certify that on this 5th day of April, 2021, a true copy of the foregoing "The Bureau of Insurance's Response To Comments" was sent by electronic mail to:

Robert Bradshaw
IIAV, PIA, NAIFA-Virginia & VAHU
8600 Mayland Drive
Richmond, Virginia 23294
rbradshaw@iiav.com

Leigh Hubbard
Virginia Land Title Association
14001 C Saint German Drive, Suite 822
Centreville, Virginia, 20121
vlta@vlta.org

Michelle Caroll Foster
American Council of Life Insurers
101 Constitution Avenue NW
Washington, DC 20001
michellefoster@acli.com

Marc Follmer
Virginia Farm Bureau Mutual Insurance Company
12580 West Creek Parkway
Richmond, Virginia 23238
marc.follmer@vafb.com

Nancy Egan
American Property Casualty Insurance Association
8700 W Bryn Mawr, Suite 1200 S
Chicago, Illinois 60631
nancy.egan@apci.org

Andrew Kirkner
National Association of Mutual Insurance Companies
36001 Vincennes Road
Indianapolis, Indiana 46268
akirkner@NAMIC.org

Wesley Bissett
Independent Agents and Brokers of America
127 South Peyton Street Fl 4
Alexandria, Virginia 22314
wes.bissett@IIABA.net

John Morris
UnitedHealthcare
10 Cadillac Drive, Suite 200
Brentwood, Tennessee 37217
john_f_morris@uhc.com

/s/ Patricia A.C. McCullagh
Patricia A.C. McCullagh

Project 6459 - Proposed

State Corporation Commission, Bureau Of Insurance

CH 430 Insurance Data Security Risk Assessment and Reporting

Chapter 430

INSURANCE DATA SECURITY RISK ASSESSMENT AND REPORTING

14VAC5-430-10. Applicability and scope.

This chapter sets forth rules to carry out the provisions of the Insurance Data Security Act, Article 2 (§ 38.2-621, et seq.) of Chapter 6 of Title 38.2 of the Code of Virginia, and sets minimum standards for risk assessment and security standards required of all licensees. However, as outlined, the specific requirements for licensees may differ in certain circumstances, depending on the size and complexity of the licensee. This chapter applies to and protects physical and electronic data, including nonpublic information, stored, transmitted, and processed across various information systems or any other media used by licensees.

14VAC5-430-20. Severability.

If any provision of this chapter or its application to any person or circumstance is for any reason held to be invalid by a court or the commission, the remainder of this chapter and the application of the provisions to other persons or circumstances shall not be affected.

14VAC5-430-30. Definitions.

The following word and terms when used in this chapter shall have the following meanings, unless context clearly indicates otherwise:

"Authorized person" means a person known to and authorized 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.

"Bureau" means the Bureau of Insurance.

"Commissioner" means the Commissioner of Insurance.

"Consumer" means an individual, including any applicant, policyholder, former policyholder, insured, beneficiary, claimant, and certificate holder, who is a resident of Virginia and whose nonpublic information is in the possession, custody, or control of a licensee or an authorized person.

"Cybersecurity event" means an event resulting in unauthorized access to, disruption of, or misuse of an information system or nonpublic information in the possession, custody, or control of a licensee or an authorized person. "Cybersecurity event" does not include (i) the unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization or (ii) an event in 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.

"Encrypted" or "encryption" means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key.

"Home state" means the jurisdiction in which the producer maintains its principal place of residence or principal place of business and is licensed by that jurisdiction to act as a resident insurance producer.

"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.

"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 or process control systems, telephone switching and private branch exchange systems, and environmental control systems.

[~~"Level one licensee" means any licensee with more than 10 employees and authorized persons.~~

~~"Level two licensee" means any licensee with 10 or fewer employees and authorized persons. A level two licensee may choose to comply with the requirements for a level one licensee. If a licensee ceases to qualify as a level two licensee, the licensee shall have 180 days from the date it ceases to qualify to comply with the requirements of a level one licensee.~~]

"Licensee" means any person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of Virginia. "Licensee" does not include a purchasing group or a risk retention group chartered and licensed in a state other than Virginia or a person that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

"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;

2. Possession factors, such as a token or text message on a mobile device; or

3. Inherence factors, such as a biometric characteristic.

"Nonpublic information" means information that is not publicly available information and is:

1. Business-related information of a licensee the tampering with which, or the 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 that because of name, number, personal mark, or other identifier can be used to identify such consumer, in any combination with a consumer's (i) social security number; (ii) driver's license number or nondriver identification card number; (iii) financial account, credit card, or debit card number; (iv) security code, access code, or password that would permit access to a consumer's financial account; (v) passport number; (vi) military identification number; or (vii) biometric records; or

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 that can be used to identify a particular consumer, and that relates to (i) the past, present, or future physical, mental, or behavioral health or condition of any consumer or a member of the consumer's family; (ii) the provision of health care to any consumer; or (iii) payment for the provision of health care to any consumer.

["Nonpublic information" does not include a consumer's personally identifiable information that has been anonymized using a method no less secure than the safe harbor method under HIPAA.

"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. 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 (i) that the information is of the type that is available to the general public and (ii) 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.]

"Third-party service provider" means a person, not otherwise defined as a licensee, that contracts with a licensee to maintain, process, or store nonpublic information or otherwise is permitted access to nonpublic information through its provision of services to the licensee, or an insurance-support organization.

14VAC5-430-40. Information security program risk assessment.

A. [~~In addition to the information security program requirements of § 38.2-623 of the Code of Virginia, each level one licensee shall conduct periodic risk assessments consistent with the objectives of the most current revision of NIST SP 800-30, NIST SP 800-39, or other substantially similar standard, taking into consideration the level one licensee's size and complexity.~~

~~1. Each level one licensee shall consider cybersecurity risks in its enterprise risk management process.~~

~~2. Compliance with the provisions of this subsection is required for all level one licensees on or before (insert date one year from the effective date of this chapter).~~

~~B.~~] In addition to the information security program requirements of § 38.2-623 of the Code of Virginia, taking into consideration the [~~level two~~] licensee's size and complexity, each [~~level two~~] licensee shall conduct a periodic risk assessment consistent with the following [~~elements~~ processes] :

1. Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration, or destruction of nonpublic information held by a [~~level two~~] licensee [including the security of information systems and nonpublic information that are accessible to, or held by third-party service providers] ;

2. Assess the likelihood and potential damage of these threats taking into consideration the sensitivity of nonpublic information in the possession, custody, or control of the licensee [~~and its authorized persons~~] ;

3. 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, such as employee training [and management] ; information classification that includes the processing, storage, transmission, and disposal of information; and the detection, prevention, and response to attacks and intrusions; and

4. Implement information safeguards to manage the threats identified in the licensee's ongoing assessment and, no less than annually, assess the effectiveness of the key controls, systems, and procedures.

[B. An assessment conducted in accordance with the objectives of the most current revision of NIST SP 800-30, NIST SP 800-39, or other substantially similar standard, shall meet the requirements for a periodic assessment in subsection A of this section.

C.] Compliance with the provisions of this subsection is required of all [~~level two~~] licensees on or before [~~July 1, 2022~~ (insert date one year from the effective date of this chapter)] .

14VAC5-430-50. Information security program security measures.

A. [~~As part of its information security program and based on its risk assessments, each level one licensee shall implement the appropriate measures consistent with NIST SP 800-53, NIST SP 800-171, or any substantially similar framework based on these standards, taking into consideration its size and complexity. Compliance with the provisions of this subsection is required for all level one licensees on or before (insert date one year from the effective date of this chapter).~~

~~B.~~] As part of its information security program and based on its risk assessments, each [~~level two~~] licensee shall implement appropriate security measures as follows:

1. Manage the data, personnel, devices, systems, and facilities of the licensee in accordance with its identified risk;

2. Protect, by encryption or other appropriate means, all nonpublic information while being transmitted over an external network;

3. Protect, by encryption or other appropriate means, all nonpublic information stored on portable computing, storage devices, or media;

4. Adopt secure development practices for applications developed in-house and used by the licensee;

5. Adopt procedures for evaluating and assessing the security of externally developed applications utilized by the licensee;

6. Implement effective controls, including multi-factor authentication, for authorized [~~individuals~~ persons] to access nonpublic information; and

7. Use audit trails or audit logs designed to detect and respond to cybersecurity events and to reconstruct material financial transactions.

[B.] Compliance with the provisions of this [~~subsection~~ section] is required of all [~~level two~~] licensees on or before [~~July 1, 2022~~ (insert date one year from the effective date of this chapter)] .

C. [Security measures implemented in accordance with the objectives of the most current revision of NIST SP 800-30, NIST SP 800-39, or other substantially similar standard, shall meet the requirements for security measures in subsection A of this section.

D.] Effective July 1, 2022, each licensee that utilizes a third-party service provider shall:

1. Exercise due diligence in selecting a third-party service provider; and

2. Require the third-party service provider to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, the third-party service provider.

14VAC5-430-60. Reporting cybersecurity events to the commissioner.

A. Reporting cybersecurity events to the commissioner.

1. Once a licensee has determined [both] that a cybersecurity event has occurred and [that] the licensee has a duty to report it to the commissioner pursuant to § 38.2-625 of the Code of Virginia, the licensee shall notify the commissioner within three business days that it has information to report, using the email address designated by the bureau. This notification should include the name, telephone number, and email address of the individual who is the licensee's designated contact for the cybersecurity event.

2. Instructions for communicating the information required by § 38.2-625 of the Code of Virginia to the commissioner through a secure portal will be provided by the bureau in response to the email.

3. The licensee shall update the commissioner on the progress of its investigation as information becomes known to the licensee until the licensee has provided [~~all~~ as much of] the information set forth in § 38.2-625 of the Code of Virginia [as possible] .

4. If also required to notify consumers [~~under § 38.2-626 of the Code of Virginia and 14VAC5-430-70~~] , licensees shall (i) provide the commissioner with a copy of the notice template and any documentation provided to consumers and (ii) maintain a list of consumers notified and retain the list for [~~the longer of five years or~~] the timeframe established by § 38.2-624 D of the Code of Virginia.

B. Except where nonpublic information has been accessed, once a domestic insurance company has notified the commissioner of the date, nature, and scope of the cybersecurity event, the [insurance] company may report [~~all~~ any] remaining information required by § 38.2-625 of the Code of Virginia [discovered by the licensee pursuant to its investigation] (i) annually in a separate report, (ii) in the certification described in § 38.2-623 H of the Code of Virginia, or (iii) on a continuing basis through the portal established for [~~the company~~ reporting cybersecurity events ~~by~~ to] the bureau [~~for this purpose~~].

C. Unless exempted by § 38.2-629 A 2 of the Code of Virginia, producers whose home state is Virginia shall report cybersecurity events to the commissioner in accordance with subsection A of this section.

D. If required to report to the commissioner, nondomestic insurance companies, and, unless exempted under § 38.2-629 A 2 of the Code of Virginia, producers whose home state is not Virginia shall notify the commissioner of the cybersecurity event pursuant to § 38.2-625 A 2 of the Code of Virginia as set forth in subsection A of this section.

14VAC5-430-70. Consumer notification provisions.

A. Licensees, except those exempted under [subsections A 1 or A 2 of] § 38.2-629 [~~A-2~~] of the Code of Virginia, that determine a cybersecurity event has occurred and has caused or has a reasonable likelihood of causing identity theft or other fraud to consumers whose information was accessed or acquired shall notify those consumers in accordance with § 38.2-626 of the Code of Virginia, subject to any applicable numerical threshold.

B. Each licensee required to notify consumers of a cybersecurity event that does not intend to notify consumers based on a belief that the cybersecurity event does not have a reasonable likelihood of causing identity theft or other fraud to the consumers shall notify the commissioner of its position and provide [~~a detailed~~ an] explanation supporting the licensee's position.

~~[C. If, upon review of the report, the cybersecurity event does have a reasonable likelihood of causing identity theft or other fraud to the consumer, the commissioner may require the licensee to notify the affected consumers in accordance with § 38.2-626 of the Code of Virginia.~~

~~]~~

Documents Incorporated by Reference (14VAC5-430)

DOCUMENTS INCORPORATED BY REFERENCE (14VAC5-430)

National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, 100 Bureau Drive (Mail Stop 8930), Gaithersburg, MD 20899-8930, sec-cert@nist.gov

NIST, Special Publication, Guide for Conducting Risk Assessments, 800-30 (rev. 1, 9/2012)

NIST, Special Publication, Managing Information Security Risk Organization, Mission, and Information System View, 800-39 (eff. 3/2011)

~~[NIST, Special Publication, Security and Privacy Controls for Federal Information Systems and Organizations, 800-53 (rev. 4, 4/2013)~~

~~NIST, Special Publication, Protecting Controlled Unclassified Information, 800-171 (rev. 2, 2/2020)]~~