REGULATORY IMPACT ANALYSIS AND TIERING STATEMENT

806 KAR 3:250

Contact Person: Abigail Gall

Phone: 502-782-5260

Email: abigail.gall@ky.gov

(1) Provide a brief summary of:

(a) What this administrative regulation does: This administrative regulation establishes the reporting process for licensees to report a cybersecurity event, or to file an exemption or compliance attestation with the department.

(b) The necessity of this administrative regulation: KRS 304.2-110(1) authorizes the Commissioner of Insurance to promulgate administrative regulations necessary for or as an aid to the effectuation of any provision of the Kentucky Insurance Code. KRS 304.3-756 requires a non-exempt licensee to develop, implement, and maintain a comprehensive information security program based on an internal risk assessment. KRS 304.3-760 requires non-exempt licensees to notify the Commissioner of Insurance of a cybersecurity event involving non-public information. KRS 304.3-766 sets forth the reporting and compliance parameters for non-exempt licensees who are deemed compliant with KRS 304.3-750 to KRS 304.3-768 due to their adherence to the provisions of the Health Insurance Portability and Accountability Act of 1996 or the Gramm-Leach-Bliley Act of 1999.

(c) How this administrative regulation conforms to the content of the authorizing statutes: KRS 304.2-110 authorizes the Commissioner of Insurance to promulgate administrative regulations necessary for or as an aid to the effectuation of any provision of the Kentucky Insurance Code, as defined in KRS 304.1-010.

(d) How this administrative regulation currently assists or will assist in the effective administration of the statutes: This administrative regulation will establish the specific reporting procedures that must be followed to ensure compliance with statutory cybersecurity requirements.

(2) If this is an amendment to an existing administrative regulation, provide a brief summary of:

(a) How the amendment will change this existing administrative regulation: This a new administrative regulation.

(b) The necessity of the amendment to this administrative regulation: This is a new administrative regulation.

(c) How the amendment conforms to the content of the authorizing statutes: This is a new administrative regulation.

(d) How the amendment will assist in the effective administration of the statutes: This is a new administrative regulation.

(3) List the type and number of individuals, businesses, organizations, or state and local governments affected by this administrative regulation: This administrative regulation would affect all insurers and business entities licensed in Kentucky. More specifically, domestic insurers and business entities who are not exempt under KRS 304.3-752.

(4) Provide an analysis of how the entities identified in question (3) will be impacted by either the implementation of this administrative regulation, if new, or by the change, if it is an amendment, including:

(a) List the actions that each of the regulated entities identified in question (3) will have to take to comply with this administrative regulation or amendment:

Insurers and businesses entities that are exempt under KRS 304.3-752 or deemed compliant under KRS 304.3-766 will need to annually file a Cybersecurity Exemption Compliance Form with the department. Those who are not exempt will need to annually file a Cybersecurity Compliance Attestation Form with the department. Entities who are deemed compliant under KRS 304.3-766 will need to submit a cybersecurity event notification to DOI.CommissionerOffice@ky.gov. Entities who are not exempt or deemed compliant under KRS 304.3-766 are required to file a Cybersecurity Event Reporting Form through their eService's account within three (3) business days of the event and to update that submission appropriately.

(b) In complying with this administrative regulation or amendment, how much will it cost each of the entities identified in question (3):

This administrative regulation should not establish any cost for entities because many of them already have an eServices account. There could be a cost associated with compliance for those who are not exempt. Some entities will be required to conduct a risk assessment, and as a result, develop an information security program. Those costs would be determined based on the size of the licensee and the amount of information held in their electronic systems.

(c) As a result of compliance, what benefits will accrue to the entities identified in question (3) Regulated entities will have met the national standard for information security programs, avoid civil penalties, and protect private consumer and business information.

(5) Provide an estimate of how much it will cost the administrative body to implement this administrative regulation:

(a) Initially: No associated cost

(b) On a continuing basis: No associated cost

(6) What is the source of the funding to be used for the implementation and enforcement of this administrative regulation: The Department of Insurance's operational budget.

(7) Provide an assessment of whether an increase in fees or funding will be necessary to implement this administrative regulation, if new, or by the change if it is an amendment: No, there is not a need to increase fees.

(8) State whether or not this administrative regulation establishes any fees or directly or indirectly increases any fees: No, this regulation does not establish any fees directly or indirectly.

(9) TIERING: Is tiering applied? (Explain why or why not) Tiering is not applied because this regulation applies equally to all entities who are required to comply with the authorizing statutes.

FISCAL NOTE

806 KAR 3:250
Contact Person: Abigail Gall
Phone: 502-782-5260
Email: abigail.gall@ky.gov

(1) What units, parts, or divisions of state or local government (including cities, counties, fire departments, or school districts) will be impacted by this administrative regulation? The Department of Insurance as the implementer.

(2) Identify each state or federal statute or federal regulation that requires or authorizes the action taken by the administrative regulation. KRS 304.2-110, 304.3-750 to KRS 304.3-768.

(3) Estimate the effect of this administrative regulation on the expenditures and revenues of a state or local government agency (including cities, counties, fire departments, or school districts) for the first full year the administrative regulation is to be in effect.

(a) How much revenue will this administrative regulation generate for the state or local government (including cities, counties, fire departments, or school districts) for the first year? No revenue will be generated.

(b) How much revenue will this administrative regulation generate for the state or local government (including cities, counties, fire departments, or school districts) for subsequent years? No revenue will be generated.

(c) How much will it cost to administer this program for the first year? There is no administrative cost associated with this program.

(d) How much will it cost to administer this program for subsequent years? There is no administrative cost associated with this program.

Note: If specific dollar estimates cannot be determined, provide a brief narrative to explain the fiscal impact of the administrative regulation.

Revenues (+/-):

Expenditures (+/-):

Other Explanation: There is no expectation of fiscal impact.

(4) Estimate the effect of this administrative regulation on the expenditures and cost savings of regulated entities for the first full year the administrative regulation is to be in effect.

(a) How much cost savings will this administrative regulation generate for the regulated entities for the first year? No cost savings are associated with this regulation.

(b) How much cost savings will this administrative regulation generate for the regulated entities for subsequent years? No cost savings are associated with this regulation.

(c) How much will it cost the regulated entities for the first year? There is no cost expected.

(d) How much will it cost the regulated entities for subsequent years? There is no cost expected.

Note: If specific dollar estimates cannot be determined, provide a brief narrative to explain the fiscal impact of the administrative regulation.

Cost Savings (+/-):

Expenditures (+/-):

Other Explanation: There is no cost associated with this administrative regulation and therefore no fiscal impact.

(5) Explain whether this administrative regulation will have a major economic impact, as defined below. *"Major economic impact" means an overall negative or adverse economic impact from an administrative regulation of five hundred thousand dollars ($500,000) or more on state or local government or regulated entities, in aggregate, as determined by the promulgating administrative bodies. [KRS 13A.010(13)]*

As per a Deloitte report, the average U.S. small business will invest between 6% and 14% of its annual IT budget on cybersecurity. This represents less than a quarter of the total budget allocated to cybersecurity. The average financial cost of a cyber attack to a U.S. small business in a 12 month period is $25,612.