Bill Summary
1st Session of the 59th Legislature

Bill No.:	**SB 543**
Version:	**CS**
Request No.:	**1928**
Author:	**Sen. Montgomery**
Date:	**02/21/2023**

Bill Analysis

SB 543 creates the Insurance Data Security Act. The measure requires each licensee of the Insurance Department to develop, implement, and maintain a comprehensive written information security program based on the risk assessment of the licensee. The licensee shall provide the assessment and designate an employee to act on behalf of the licensee who is responsible for the information security program. The program shall be designed to address risks identified in the assessment, design security measures addressing areas of access and auditing systems, remain informed of developments in cybersecurity, and train personnel.

The measure requires any board of directors licensed by the Department to implement, oversee, and/or delegate oversight of the program within 1 year of the effective date. Third-party vendors must be chosen with due diligence. Licensees shall also be required to establish a written incident response plan for any cybersecurity event. Insurers shall be required to submit a written statement affirming their compliance with the provisions of this measure before March 1 of each year as well as maintain records for examination by the Department for a period not less than 5 years. Records submitted to the Commissioner shall be kept confidential and are not subject to the Oklahoma Open Records Act. The Commissioner is authorized to share records and information if needed with relevant state, federal, and international regulatory agencies as well as the National Association of Insurance Commissioners and its affiliates.

If a cybersecurity event occurs, the licensee must conduct a prompt investigation of the event and maintain a record of the event for no less than 5 years. A cybersecurity event shall not include the unauthorized acquisition of encrypted nonpublic information if the encryption, process, or key is not also acquired, released, or used without authorization. The Commissioner must be notified within 3 days of a cybersecurity event occurring as well as how the event was discovered and occurred. If nonpublic information was accessed, the licensee shall comply with the notification provisions provided for by the Security Breach Notification Act.

The measure exempts any licensee with less than $5 million in gross annual revenue or subject to the Health Insurance Portability and Accountability Act from the provisions of this measure. Licensees that lose their exemption status shall have 180 days to comply with the provisions of this measure.

Prepared by: Kalen Taylor