OLR Bill Analysis

sHB 6607

AN ACT INCENTIVIZING THE ADOPTION OF CYBERSECURITY STANDARDS FOR BUSINESSES.

SUMMARY

This bill establishes an affirmative defense for civil action brought against a covered entity (see below) for a data breach of personal or restricted information. If the action alleges the breach resulted from a covered entity's failure to implement reasonable cybersecurity controls, the entity has an affirmative defense if it created, maintained, and complied with a written cybersecurity program containing administrative, technical, and physical safeguards for the protection of personal or restricted information. To qualify as an affirmative defense, these cybersecurity programs must (1) meet specified design requirements and (2) conform to an industry-recognized cybersecurity framework.

Under the bill, "covered entities" are businesses accessing, maintaining, communicating, or processing personal or restricted information in or through systems, networks, or services located inside or outside the state.

EFFECTIVE DATE: October 1, 2021

CYBERSECURITY PROGRAM DESIGN REQUIREMENTS

To qualify as an affirmative defense, the bill requires that a covered entity's cybersecurity program be designed to protect the security and confidentiality of personal and restricted information. The program must specifically protect this information against (1) anticipated threats or hazards to its security or integrity and (2) unauthorized access and acquisition likely to cause material risk of identity theft or other fraud.

The bill requires the scale and scope of a covered entity's

cybersecurity program to be based on the:

1. entity's size and complexity, available resources, and nature and scope of its activities;

2. sensitivity of the information to be protected; and

3. cost and availability of tools to improve information security and reduce vulnerabilities.

INDUSTRY-RECOGNIZED CYBERSECURITY FRAMEWORKS

Under the bill, an industry-recognized cybersecurity framework includes the most current version of:

1. one or any combination of six specifically recognized frameworks (see Table 1),

2. one of four specified federal laws and regulations (for entities regulated by any of these laws or the state or federal government; see Table 2), or

3. the "Payment Card Industry Data Security Standard" in combination with one of the acceptable frameworks mentioned in Table 1 below.

Table 1: Industry-Recognized Cybersecurity Frameworks

Publisher	***Framework***
National Institute of Standards and Technology	1. "Framework for Improving Critical Infrastructure Cybersecurity" 2. Special Publication (SP) 800-171 3. SP 800-53 and 800-53a
Federal Risk and Management Program	4. "FedRAMP Security Assessment Framework"
Center for Internet Security	5. "Center for Internet Security Critical Security Controls for Effective Cyber Defense"
International Organization for Standardization and the International	6. "ISO/IEC 27000-series"

Electrotechnical Commission	

Table 2: Federal Cybersecurity Laws and Regulations

Citation	*Law or Regulation*
P.L. 104-191; 45 C.F.R. 164 (Subpart C)	Security requirements of the Health Insurance Portability and Accountability Act of 1996
P.L. 106-102	Title V of the Gramm-Leach-Bliley Act of 1999
P.L. 113-283	Federal Information Security Modernization Act of 2014
45 C.F.R. 162	Security requirements of the Health Information Technology for Economic and Clinical Health Act

The bill requires a covered entity whose cybersecurity program conforms with any of the acceptable cybersecurity frameworks to conform with revisions to these frameworks within 60 days after the revised document is published. Similarly, a covered entity whose cybersecurity program conforms with any of the specified federal cybersecurity laws or regulations must conform to any amendments within the same time period. For a covered entity that conforms to the Payment Card Industry Data Security Standard, the allowable time period to conform with a published revision is one year after the revision's publication date.

DEFINITIONS

Businesses

Under the bill, a covered entity's business type may include an individual or a sole proprietorship, partnership, firm, corporation, trust, limited liability company or partnership, joint stock company, joint ventures, associations, or other legal entities through which for-profit or non-profit business is conducted.

Data Breach

The bill defines a "data breach" as unauthorized access to and

acquisition of computerized data that (1) compromises the security or confidentiality of personal or restricted information owned by or licensed to a covered entity and (2) causes a material risk of identity theft or other fraud to a person or property (or reasonably is believed to have caused or will cause such risk). The definition specifically excludes:

1. employees or agents of a covered entity acquiring personal or restricted information in good faith for the purposes of the entity, so long as the entity does not unlawfully use this information or subject it to further unauthorized disclosure, or

2. the acquisition of this information pursuant to a (a) search warrant, (b) subpoena or other court order, or (c) regulatory state agency's order or duty.

Personal and Restricted Information

Under the bill, "personal information" means an individual's name (i.e., first name or initial and last name) in combination with or linked to one or more specified unencrypted, unredacted, or unaltered data elements. These data elements are social security numbers; driver's license or state identification numbers; and account or credit or debit card numbers in combination with and linked to a required security code, access code, or password permitting access to an individual's financial account.

"Restricted information" means any unencrypted, unredacted, or unaltered information about an individual that, alone or in combination with other information (including personal information as described above), (1) can be used to distinguish or trace the individual's identity or is linked or linkable to an individual and (2) is likely to result in a material risk of identity theft or other fraud to a person or property if breached. The definition excludes personal information.

COMMITTEE ACTION

Commerce Committee

Joint Favorable Change of Reference - JUD
Yea 22 Nay 1 (03/22/2021)

Judiciary Committee

Joint Favorable Substitute
Yea 32 Nay 3 (04/09/2021)