Amend **CSHB 8** (house committee report) as follows:

(1) Strike page 3, line 18, through page 5, line 12.

(2) On page 13, lines 11 and 12, strike "and 2054.518" and substitute "2054.518, and 2054.519".

(3) On page 17, strike lines 9 and 10 and substitute the following:

resources technology for a state agency at a cost to the agency of $1 million or more is responsible for addressing known cybersecurity risks associated with the technology and is responsible for any cost associated with addressing the identified cybersecurity risks. For a major information resources project, the vendor shall provide to state agency contracting personnel:

(4) On page 17, on both lines 14 and 21, between "2054.516" and the underlined semicolon, insert "or Section 2054.517".

(5) On page 17, line 24, between "risks" and the underlined period, insert "as identified in collaboration with this state following a risk assessment".

(6) On page 17, between lines 24 and 25, insert the following:

Sec. 2054.519. CYBERSECURITY RISKS AND INCIDENTS. (a) The department shall develop a plan to address cybersecurity risks and incidents in this state. The department may enter into an agreement with a national organization, including the National Cybersecurity Preparedness Consortium, to support the department's efforts in implementing the components of the plan for which the department lacks resources to address internally. The agreement may include provisions for:

(1) providing fee reimbursement for appropriate industry-recognized certification examinations for and training to state and local officials and first responders preparing for and responding to cybersecurity risks and incidents;

(2) developing and maintaining a cybersecurity risks and incidents curriculum using existing programs and models for training state and local officials and first responders;

(3) delivering to state agency personnel with access to state agency networks routine training related to appropriately protecting and maintaining information technology systems and

devices, implementing cybersecurity best practices, and mitigating cybersecurity risks and vulnerabilities;

(4) providing technical assistance services to support preparedness for and response to cybersecurity risks and incidents;

(5) conducting cybersecurity training and simulation exercises for state agencies, political subdivisions, and private entities to encourage coordination in defending against and responding to cybersecurity risks and incidents;

(6) assisting state agencies and political subdivisions in developing cybersecurity information-sharing programs to disseminate information related to cybersecurity risks and incidents; and

(7) incorporating cybersecurity risk and incident prevention and response methods into existing state and local emergency plans, including continuity of operation plans and incident response plans.

(b) In implementing the provisions of the agreement prescribed by Subsection (a), the department shall seek to prevent unnecessary duplication of existing programs or efforts of the department or another state agency.

(c) In selecting an organization under Subsection (a), the department shall consider the organization's previous experience in conducting cybersecurity training and exercises for state agencies and political subdivisions.

(d) The department shall consult with institutions of higher education in this state when appropriate based on an institution's expertise in addressing specific cybersecurity risks and incidents.

(7) On page 20, line 9, between "(d)" and "Not", insert the following:

A state agency may not under any circumstance sell:

(1) a person's precise geographic location information;

(2) a person's Internet browsing history;

(3) a person's application usage history; or

(4) the functional equivalent of the information

described in Subdivisions (1)-(3).

(e)

(8) Renumber the SECTIONS of the bill accordingly.