Amend **SB 1910** (house committee report) as follows:

(1) On page 1, line 10, strike "shall" and substitute "may".

(2) On page 1, line 11, strike "audited" and substitute "assessed".

(3) On page 1, strike lines 15-20, and substitute the following:

Sec. 2054.136. DESIGNATED INFORMATION SECURITY OFFICER. Each state agency shall designate an information security officer who:

(1) reports to the agency's executive level management;

(2) has authority over information security for the entire agency;

(3) possesses the training and experience required to perform the duties required by department rules; and

(4) to the extent feasible, has information security duties as the officer's primary duties.

(4) On page 1, line 22, strike "Section 2054.516" and substitute "Sections 2054.516 and 2054.517".

(5) On page 1, line 24, between "agency" and "implementing", insert ", other than an institution of higher education subject to Section 2054.517,".

(6) On page 2, strike lines 1-22, and substitute the following:

website or mobile application that processes any sensitive personally identifiable or confidential information must:

(1) submit a biennial data security plan to the department not later than October 15 of each even-numbered year, to establish planned beta testing for websites or applications; and

(2) subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test.

(7) On page 2, line 23, strike "(c)" and substitute "(b)".

(8) On page 2, between lines 26 and 27, insert the following:

Sec. 2054.517. DATA SECURITY PROCEDURES FOR ONLINE AND MOBILE APPLICATIONS OF INSTITUTIONS OF HIGHER EDUCATION. (a) Each institution of higher education, as defined by Section 61.003, Education Code, shall adopt and implement a policy for Internet website and mobile application security procedures that complies with this section.

(b) Before deploying an Internet website or mobile application that processes confidential information for an institution of higher education, the developer of the website or application for the institution must submit to the institution's information security officer the information required under policies adopted by the institution to protect the privacy of individuals by preserving the confidentiality of information processed by the website or application. At a minimum, the institution's policies must require the developer to submit information describing:

(1) the architecture of the website or application;

(2) the authentication mechanism for the website or application; and

(3) the administrator level access to data included in the website or application.

(c) Before deploying an Internet website or mobile application described by Subsection (b), an institution of higher education must subject the website or application to a vulnerability and penetration test conducted internally or by an independent third party.

(d) Each institution of higher education shall submit to the department the policies adopted as required by Subsection (b). The department shall review the policies and make recommendations for appropriate changes.