BILL ANALYSIS

C.S.H.B. 2004
By: McCall
State Affairs
Committee Report (Substituted)

BACKGROUND AND PURPOSE

As emerging technologies increase the availability and transferability of data, the challenges of protecting confidential data from misappropriation multiply rapidly. Privacy breaches make headlines and affect citizen trust in government's ability to safeguard their confidential information. Once data is exposed, it can be replicated and sold countless times, and ultimately confidentiality can be impossible to restore. Factors, such as lost or stolen equipment and accidental exposure from posting social security numbers to an Internet site or e-mailing personally identifying information to the wrong party, exceed hacking as the primary source of data loss. Texas law governing breaches of system security does not adequately cover information held by state or local government entities.

C.S.H.B. 2004 provides for notification by a state agency or local government of persons affected by a security breach, to the same extent such notice is required to be given by a person who conducts business in Texas.

RULEMAKING AUTHORITY

It is the committee's opinion that this bill does not expressly grant any additional rulemaking authority to a state officer, department, agency, or institution.

ANALYSIS

C.S.H.B 2004 amends the Government Code and the Local Government Code, respectively, to require a state agency or local government that owns, licenses, or maintains computerized data that includes sensitive personal information to comply, in the event of a breach of system security, with the notification requirements set forth by provisions of the Business & Commerce Code, to the same extent as a person who conducts business in Texas.

C.S.H.B. 2004 amends the Business & Commerce Code to expand the definition of "sensitive personal information" to include information that identifies an individual and relates to the physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual. The bill redefines "breach of system security" to clarify that the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person includes data that is encrypted, if the person accessing the data has the key required to decrypt the data.

EFFECTIVE DATE

September 1, 2009.

COMPARISON OF ORIGINAL AND SUBSTITUTE

C.S.H.B. 2004 adds provisions, not in the original, to amend the Business & Commerce Code to

redefine "sensitive personal information" and "breach of system security."

C.S.H.B. 2004, rather than adding a chapter to the Government Code relating to security breach notification by a state agency or local government, amends the Information Resource Management Act in the Government Code to add provisions relating to security breach notification by a state agency, and amends provisions in the Local Government Code relating to electronic storage of records to add provisions relating to security breach notification by a local government.

C.S.H.B. 2004 defines "sensitive personal information" and "breach of system security" in its Government Code provisions by reference to the definitions the substitute adds to the Business & Commerce Code, and defines the two terms separately in the Local Government Code, also by reference to the added definitions in the Business & Commerce Code, whereas the original contains express definitions of the two terms in the new chapter it adds and does not reference other definitions.

C.S.H.B. 2004 removes the definitions of "state agency" and "local government" as contained in the original.

C.S.H.B. 2004 in its definitions of "sensitive personal information" includes information that identifies an individual and relates to the physical or mental health or condition of the individual, the provision of health care to the individual, or payment for the provision of health care to the individual, whereas the original does not.

C.S.H.B. 2004 removes the original's inclusion, within the definition of "sensitive personal information," of names and items that are encrypted and for which the person accessing the information has access to the key required to decrypt the information. The substitute, unlike the original, includes the unauthorized acquisition of date that is encrypted, if the person accessing the data has the key required to decrypt the data, within the definition of "breach of system security."

C.S.H.B. 2004, like the original, includes in the definition of "breach of system security" an unauthorized acquisition of computerized data that compromises the security of confidentiality of sensitive personal information, but unlike the original, also includes the unauthorized acquisition of computerized data that compromises the integrity of sensitive personal information.

C.S.H.B. 2004 in the definition of "breach of system security" refers to sensitive personal information maintained by a person, whereas the original in its definition of the term refers to sensitive personal information maintained by a state agency or local government.

C.S.H.B. 2004 provides that good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner, whereas the original provides that good faith acquisition by an employee, contractor, or agent of the state agency or local government, for the purposes of the state agency or local government, is not a breach unless the employee, contractor, or agency uses or discloses the sensitive personal information in an unauthorized manner.

C.S.H.B. 2004 requires a state agency or local government that owns, licenses, or maintains computerized data that includes sensitive personal information to comply, in the event of a breach of system security, with notification requirements of the Business & Commerce Code to the same extent as a person who conducts business in Texas, whereas the original refers only to owning or licensing of data, and not to maintaining data, and includes new notification provisions, absent from the substitute, with which the agency or local government must comply.