SUBJECT: Modifying applicability and scope of sensitive data breach requirements

COMMITTEE: State Affairs — committee substitute recommended

VOTE: 13 ayes — Paddie, Hernandez, Deshotel, Harless, Howard, Hunter, P. King, Lucio, Metcalf, Raymond, Shaheen, Slawson, Smithee

0 nays

WITNESSES: For — (*Registered, but did not testify*: Hope Osborn, Texas 2036)

Against — None

On — (*Registered, but did not testify*: Ender Reed, Harris County Commissioners Court; Nancy Rainosek, Texas Department of Information Resources)

BACKGROUND: Government Code sec. 2054.1125 requires a state agency that owns, licenses, or maintains computerized data that includes certain sensitive information, in the event of a breach or suspected breach of system security or an unauthorized exposure of that information, to comply with the notification requirements specified in other law to the same extent as someone who conducts business in Texas. Such agencies also must notify the Department of Information Resources, including the chief information security officer, within 48 hours of the discovery of the breach, suspected breach, or unauthorized exposure.

Some have noted that local governments are not required to report cyberattacks to the Department of Information Resources, which reduces the state's ability to track and respond to cyberattacks at the local level.

DIGEST: CSHB 4395 would make the notification requirements of Government Code sec. 2054.1124 applicable to local governments that owned, licensed, or maintained computerized data that included sensitive personal information, confidential information, or information the disclosure of which was regulated by law.

A state agency or local government subject to the notification requirements would have to comply with all DIR rules relating to security incidents.

The bill also would expand the list of incidents that required notification of the Department of Information Resources (DIR) by state agencies and local governments. The bill would replace statutory references to a "breach" or "event" with references to "security incidents," and would define “security incident” as the actual or suspected unauthorized access, disclosure, exposure, modification, or destruction of sensitive personal information, confidential information, or other information the disclosure of which was regulated by law. This would include a security breach or suspected breach and ransomware.

The bill would take effect September 1, 2021.