

## **BILL ANALYSIS**

C.S.H.B. 712  
By: Shaheen  
State Affairs  
Committee Report (Substituted)

### **BACKGROUND AND PURPOSE**

Cybersecurity attacks are increasing, particularly among local governments. While state agencies are required to report these incidents to the Department of Information Resources (DIR), which oversees cybersecurity for the State of Texas, local governments are not. As such, DIR only learns of incidents at the local level when local governments choose to report them. This is concerning because the state cannot respond or track accurate data when incidents are not reported to DIR. C.S.H.B. 712 seeks to ensure that cybersecurity incidents at all levels of government in Texas are reported to DIR so that the state has the ability to track patterns, collect accurate data, and help mitigate damage to governmental entities experiencing such a security incident.

### **CRIMINAL JUSTICE IMPACT**

It is the committee's opinion that this bill does not expressly create a criminal offense, increase the punishment for an existing criminal offense or category of offenses, or change the eligibility of a person for community supervision, parole, or mandatory supervision.

### **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. 712 amends the Government Code to revise the scope of provisions governing security breach notification procedures for applicable state agencies as follows:

- expands the incidents that require notification to include all security incidents, defined by the bill as a breach or suspected breach of system security and the introduction of ransomware into a computer, computer network, or computer system;
- makes the provisions applicable also to local governments that own, license, or maintain computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law;
- requires a state agency or local government subject to the notification procedures to comply with all Department of Information Resources (DIR) rules relating to reporting security incidents in the event of such an incident; and
- makes the provisions inapplicable to a security incident that a local government is required to report to ERCOT.

### **EFFECTIVE DATE**

September 1, 2023.

## **COMPARISON OF INTRODUCED AND SUBSTITUTE**

While C.S.H.B. 712 may differ from the introduced in minor or nonsubstantive ways, the following summarizes the substantial differences between the introduced and committee substitute versions of the bill.

The substitute narrows the scope of the definition of "security incident." Whereas the introduced defined the term 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 is regulated by law, including a breach or suspected breach of system security or the introduction of ransomware into a computer, computer network, or computer system, the substitute defines the term only as a breach or suspected breach of system security or the introduction of ransomware into a computer, computer network, or computer system.

The introduced required a state agency or local government subject to the notification procedures to comply with all DIR rules relating to security incidents in the event of such an incident. The substitute specifies that the rules with which the agency or local government must comply are the DIR rules relating to reporting security incidents.

The substitute includes a provision absent from the introduced making the notification requirements inapplicable to a security incident that a local government is required to report to ERCOT.