BILL ANALYSIS

Senate Research Center

S.B. 271
By: Johnson
Business & Commerce
5/24/2023
Enrolled

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

Current state law only requires certain institutions—state agencies, institutions of higher education, school districts, charter schools, and election officials—to report certain types of security incidents to the Texas Department of Information Resources (DIR) within 48 hours. However, the institutions that are covered by state law and the type of security incidents that are required to be reported do not provide an accurate portrayal of the current cyber threat landscape.

Under current law, cities and counties are not required to report cyberattacks to the state. Additionally, the current definition of "security incident" that state agencies are required to report only cover attacks where a data breach occurs.

This limited reporting of cybersecurity incidents creates an inaccurate portrayal of the cyber threat landscape in Texas. The state's inconsistent requirements for reporting of cybersecurity incidents can hinder tracking trends and patterns, and complicate understanding the scope and complexity of cyberattacks. The gaps in our understanding of current and potential cyber threats leave the state vulnerable to future attacks, resulting in costly responses and recovery efforts.

Important provisions of S.B. 271:

- Clarify the current definition of "security incident" to incorporate cyberattacks that do not involve a data breach, such as a distributed denial of service (DDoS) attack.
- Require local entities to report security incidents to DIR in the same manner as state agencies.

Committee Substitute for S.B. 271

C.S.S.B. 271 addresses concerns from local entities surrounding the reporting of security incidents. There are three main changes in the committee substitute.

1. The filed bill would have expanded the definition of the security incidents that state agencies and locals entities reportable to DIR to include: involving 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 as defined by Section 521.053, Business & Commerce Code; and the introduction of ransomware, as defined by Section 33.023, Penal Code, into a computer, computer network, or computer system.

   The committee substitute now defines a security incident as a breach or suspected breach as defined by Section 521.053, Business & Commerce Code; and the introduction of ransomware, as defined by Section 33.023, Penal Code, into a computer, computer network, or computer system. These changes are to address stakeholder concerns around the amount of incidents that would be required to be reported to DIR.

2. The committee substitute also clarifies that the state agencies and local entities have to comply with rules relating to reporting security incidents under this section. This language was added to provide clarification to local entities that they are not subject to all

of DIR's rules regarding security incidents, but only those that relate to the reporting of incidents under this section.

3. Last, the committee substitute exempts local governments subject to mandatory reporting requirements for security incidents to the independent organization certified by the Public Utility Commission of Texas pursuant to Section 39.151, Utilities Code. This language applies to local electric providers that are subject to ERCOT's reporting requirements. These entities are already complying with the intent of this legislation and if a security incident were to occur at a municipal utility, ERCOT has the expertise to respond and provide remediation.

These changes attempt to address local entities' concerns while preserving the intent of the bill to ensure that the state receives reporting from local entities and that DIR can offer support to a local entity after a cyber incident in a timely manner.

S.B. 271 amends current law relating to state agency and local government security incident procedures.

RULEMAKING AUTHORITY

This bill does not expressly grant any additional rulemaking authority to a state officer, institution, or agency.

SECTION BY SECTION ANALYSIS

SECTION 1. Transfers Section 2054.1125, Government Code, to Subchapter R, Chapter 2054, Government Code, redesignates it as Section 2054.603, Government Code, and amends it, as follows:

Sec. 2054.603. New heading: SECURITY INCIDENT NOTIFICATION BY STATE AGENCY OR LOCAL GOVERNMENT. (a) Defines "security incident." Deletes existing definition of "breach of system security."

(b) Requires a state agency or local government that owns, licenses, or maintains computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law, in the event of a security incident, rather than breach or suspected breach of system security or an unauthorized exposure of that information, to:

(1) makes a nonsubstantive change to this subdivision;

(2) not later than 48 hours after the discovery of the security incident, notify:

(A) makes no changes to this paragraph; or

(B) if the security incident involves election data, the secretary of state; and

(3) comply with all Department of Information Resources (DIR) rules relating to security incidents as required by this section.

Makes conforming changes.

(c) Requires a state agency or local government, not later than the 10th business day after the date of the eradication, closure, and recovery from a security incident, to notify DIR, including the chief information security officer, of the details of the security incident, rather than event, and include in the notification an analysis of the cause of the security incident. Makes conforming changes.

(d) Provides that this section does not apply to a security incident that a local government is required to report to an independent organization certified by the Public Utility Commission of Texas under Section 39.151 (Essential Organizations), Utilities Code.

SECTION 2. Effective date: September 1, 2023.