

BILL ANALYSIS

Senate Research Center
88R15835 SCP-F

C.S.S.B. 621
By: Parker
Business & Commerce
3/14/2023
Committee Report (Substituted)

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

The Texas Department of Information Resources (DIR) is responsible for providing the state's technology infrastructure with strategic direction, coordination, leadership, and protection from cybersecurity threats. Among other duties, DIR oversees the state information security program, develops security standards and procedures for state agencies, provides incident response to state and local entities after a cybersecurity incident, provides assessment services and penetration testing to ensure security programs are operating effectively, and operates the end-user cybersecurity training program for state and local employees. DIR also provides education and certification testing for state cybersecurity professionals, and specific training to state and local entities on various aspects of cybersecurity – such as incident response – so they are prepared for addressing the many security risks that state and local security professionals face. DIR's chief information security officer (CISO) oversees the development and implementation of these programs, but this important role is not defined in state statute.

C.S.S.B. 621 would amend the Government Code of the State of Texas to mandate that the executive director employ the position of chief information security officer (CISO) in the Department of Information Resources. The CISO would be responsible for overseeing cybersecurity matters for the state, including implementing certain duties as defined by Section 2054.059, responding to reports as outlined in Section 2054.1125, developing a statewide information security framework, overseeing the development of statewide information security policies and standards, providing information security leadership and coordination, and providing strategic direction to the network security center and statewide technology centers. The CISO would also be required to submit a written report on the status and effectiveness of the state information security program to various officials and legislative committees as outlined in Section 2054.0591. The act would take effect on September 1, 2023.

C.S.S.B. 621 amends current law relating to the position of chief information security officer in the Department of Information Resources.

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. Amends Subchapter N-1, Chapter 2054, Government Code, by adding Section 2054.510, as follows:

Sec. 2054.510. CHIEF INFORMATION SECURITY OFFICER. (a) Defines "state information security program."

(b) Requires the executive director of the Texas Department of Information Resources, using existing funds, to employ a chief information security officer.

(c) Requires the chief information officer to oversee cybersecurity matters for this state including:

- (1) implementing the duties described by Section 2054.059 (Cybersecurity);
- (2) responding to reports received under Section 2054.1125 (Security Breach Notification by State Agency);
- (3) developing a statewide information security framework;
- (4) overseeing the development of statewide information security policies and standards;
- (5) developing, in coordination with state agencies, local governmental entities, and other entities operating or exercising control over state information systems or state-controlled data, information security policies, standards, and guidelines to strengthen this state's cybersecurity;
- (6) overseeing the implementation of the policies, standards, and guidelines developed under Subdivisions (3), (4), and (5);
- (7) providing information security leadership, strategic direction, and coordination for the state information security program; and
- (8) providing strategic direction to:
 - (A) the network security center established under Section 2059.101 (Network Security Center); and
 - (B) statewide technology centers operated under Subchapter L (Statewide Technology Centers), and
- (9) overseeing the preparation and submission of the report described by Section 2054.0591 (Cybersecurity Report).

SECTION 2. Effective date: September 1, 2023.