BILL ANALYSIS

C.S.S.B. 621
By: Parker
State Affairs
Committee Report (Substituted)

BACKGROUND AND PURPOSE

The 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 currently employs a chief information security officer (CISO) to oversee the development and implementation of these programs, but this important role is not defined in state statute. C.S.S.B. 621 seeks to codify the position of CISO in statute and to set out the required duties for this position.

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.S.B. 621 amends the Government Code to require the executive director of the Department of Information Resources (DIR), using existing funds, to employ a chief information security officer (CISO) to oversee cybersecurity matters for the state. The bill requires the CISO to do the following as part of that oversight:

- implement DIR's cybersecurity duties;
- respond to reports sent to DIR by state agencies regarding a breach or suspected breach of system security or an unauthorized exposure of sensitive personal or confidential information;
- develop a statewide information security framework;
- oversee the development of statewide information security policies and standards;
- collaborate with applicable state agencies, local governmental entities, and other entities operating or exercising control over state information systems or state-controlled data to strengthen the state's cybersecurity and information security policies, standards, and guidelines;

- oversee the implementation of the information security policies, standards, guidelines, and framework developed under the bill;
- provide information security leadership, strategic direction, and coordination for the state information security program;
- provide strategic direction to the network security center and statewide technology centers; and
- oversee the preparation and submission of the cybersecurity report.

For purposes of the bill's provisions, "state information security program" means the policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, services, and resources that establish the information resources security function for the state.

EFFECTIVE DATE

September 1, 2023.

COMPARISON OF SENATE ENGROSSED AND SUBSTITUTE

While C.S.S.B. 621 may differ from the engrossed in minor or nonsubstantive ways, the following summarizes the substantial differences between the engrossed and committee substitute versions of the bill.

The substitute replaces the provision in the engrossed requiring the CISO to develop, in coordination with applicable 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 the state's cybersecurity with a provision requiring the CISO to collaborate with those same agencies and entities to strengthen the state's cybersecurity and information security policies, standards, and guidelines.