BILL ANALYSIS

C.S.H.B. 3112
By: Tepper
Delivery of Government Efficiency
Committee Report (Substituted)

BACKGROUND AND PURPOSE

The bill author has informed the committee that cyber attacks can compromise the confidentiality, integrity, and availability of public records and meetings, posing a significant threat to transparency and accountability in government operations, and that certain cities have requested legislation that ensures the confidentiality of certain deliberations and records regarding cybersecurity measures. C.S.H.B. 3112 addresses these issues by establishing that a governmental body is not required to conduct an open meeting to deliberate cybersecurity measures, policies, or contracts relating to the protection of critical infrastructure and exempting certain cybersecurity information from the public availability requirement of state public information law. The bill also requires a governmental body that is required to disclose covered information to notify each person who owns and is the subject of the information.

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. 3112 amends the Government Code to establish that state open meetings law does not require a governmental body to conduct an open meeting to deliberate a cybersecurity measure, policy, or contract solely intended to protect a critical infrastructure facility located in the jurisdiction of the governmental body.

C.S.H.B. 3112 excepts information from the public availability requirement of state public information law if the information relates to the following:

- a cybersecurity measure, policy, or contract solely intended to protect a critical infrastructure facility located in the jurisdiction of the governmental body;
- coverage limits and deductible amounts for insurance or other risk mitigation coverages acquired for the protection of information technology systems, critical infrastructure, operational technology systems, or data of a governmental body or the amount of money set aside by a governmental body to self-insure against those risks;
- cybersecurity incident information reported pursuant to state law; and
- network schematics, hardware and software configurations, or encryption information or information that identifies the detection, investigation, or response practices for suspected or confirmed cybersecurity incidents if the disclosure of such information would facilitate unauthorized access to data or information, whether physical or virtual,

or to information technology resources, including a governmental body's existing or proposed information technology system.

The bill authorizes a governmental body to disclose such confidential information to comply with applicable state or federal law or a court order. The bill requires a governmental body that is required to disclose such information to retain all existing labeling on the information being disclosed and to provide notice of the required disclosure, not later than the fifth business day before the date the information is disclosed, to a person who owns the information and to a person who is the subject of the information.

C.S.H.B. 3112 defines the following terms:

- "critical infrastructure facility" as a communication infrastructure system, cybersecurity system, electric grid, electrical power generating facility, substation, switching station, electrical control center, natural gas and natural gas liquids gathering, processing, and storage transmission and distribution system, hazardous waste treatment system, water treatment facility, water intake structure, wastewater treatment plant, pump station, or water pipeline and related support facility, equipment, and property; and
- "cybersecurity" as the measures taken to protect a computer, a computer network, a computer system, or other technology infrastructure against unauthorized use or access.

EFFECTIVE DATE

On passage, or, if the bill does not receive the necessary vote, September 1, 2025.

COMPARISON OF INTRODUCED AND SUBSTITUTE

While C.S.H.B. 3112 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 includes a requirement absent from the introduced for a governmental body that is required to disclose certain information to retain all existing labeling on the information being disclosed and to provide notice of that required disclosure to applicable persons not later than the fifth business day before the date the information is disclosed.