

By: Tepper

H.B. No. 3112

Substitute the following for H.B. No. 3112:

By: Capriglione

C.S.H.B. No. 3112

A BILL TO BE ENTITLED

AN ACT

relating to the application of the open meetings law and public information law to government information related to certain cybersecurity measures.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Subchapter D, Chapter 551, Government Code, is amended by adding Section 551.0761 to read as follows:

Sec. 551.0761. DELIBERATION REGARDING CRITICAL INFRASTRUCTURE FACILITY; CLOSED MEETING. (a) In this section:

(1) "Critical infrastructure facility" means 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.

(2) "Cybersecurity" means the measures taken to protect a computer, a computer network, a computer system, or other technology infrastructure against unauthorized use or access.

(b) This chapter 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.

SECTION 2. Subchapter C, Chapter 552, Government Code, is amended by adding Section 552.1391 to read as follows:

Sec. 552.1391. EXCEPTION: CONFIDENTIALITY OF CYBERSECURITY MEASURES. (a) In this section:

(1) "Critical infrastructure facility" has the meaning assigned by Section 551.0761.

(2) "Cybersecurity" has the meaning assigned by Section 551.0761.

(b) Information is excepted from the requirements of Section 552.021 if it is information that relates to:

(1) a cybersecurity measure, policy, or contract solely intended to protect a critical infrastructure facility located in the jurisdiction of the governmental body;

(2) 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;

(3) cybersecurity incident information reported pursuant to state law; and

(4) 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

1 such information would facilitate unauthorized access to:

2 (A) data or information, whether physical or  
3 virtual; or

4 (B) information technology resources, including  
5 a governmental body's existing or proposed information technology  
6 system.

7 (c) A governmental body may disclose information made  
8 confidential by this section to comply with applicable state or  
9 federal law or a court order. A governmental body that is required  
10 to disclose information described by Subsection (b) shall:

11 (1) not later than the fifth business day before the  
12 date the information is disclosed, provide notice of the required  
13 disclosure to:

14 (A) a person who owns the information; and

15 (B) a person who is the subject of the  
16 information; and

17 (2) retain all existing labeling on the information  
18 being disclosed.

19 SECTION 3. This Act takes effect immediately if it receives  
20 a vote of two-thirds of all the members elected to each house, as  
21 provided by Section 39, Article III, Texas Constitution. If this  
22 Act does not receive the vote necessary for immediate effect, this  
23 Act takes effect September 1, 2025.