By: Capriglione H.B. No. 4231

A BILL TO BE ENTITLED

AN ACT

relating to cybersecurity for retail public utilities that provide water or sewer service.

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

SECTION 1. Section 2054.0525, Government Code, is amended to read as follows:

Sec. 2054.0525. CUSTOMERS ELIGIBLE FOR DEPARTMENT SERVICES. If the executive director determines that participation is in the best interest of this state, the following entities are eligible customers for services the department provides:

(1) a state agency;

(2) a local government;

(3) the legislature or a legislative agency;

(4) the supreme court, the court of criminal appeals, or a court of appeals;

(5) a public hospital owned or operated by this state or a political subdivision or municipal corporation of this state, including a hospital district or hospital authority;

(6) an independent organization certified under Section 39.151, Utilities Code, for the ERCOT power region;

(7) the Texas Permanent School Fund Corporation;

(8) an assistance organization, as defined by Section 2175.001;

(9) an open-enrollment charter school, as defined by

Section 5.001, Education Code;

(10) a private school, as defined by Section 5.001, Education Code;

(11) a private or independent institution of higher education, as defined by Section 61.003, Education Code;

(12) a public safety entity, as defined by 47 U.S.C. Section 1401;

(13) a volunteer fire department, as defined by Section 152.001, Tax Code; [~~and~~]

(14) a governmental entity of another state; and

(15) a retail public utility, as defined by Section 13.002, Water Code.

SECTION 2. Section 2059.058, Government Code, is amended to read as follows:

Sec. 2059.058. AGREEMENT TO PROVIDE NETWORK SECURITY SERVICES TO ENTITIES OTHER THAN STATE AGENCIES. In addition to the department's duty to provide network security services to state agencies under this chapter, the department by agreement may provide network security services to:

(1) each house of the legislature and a legislative agency;

(2) a local government;

(3) the supreme court, the court of criminal appeals, or a court of appeals;

(4) a public hospital owned or operated by this state or a political subdivision or municipal corporation of this state, including a hospital district or hospital authority;

(5) the Texas Permanent School Fund Corporation;

(6) an open-enrollment charter school, as defined by Section 5.001, Education Code;

(7) a private school, as defined by Section 5.001, Education Code;

(8) a private or independent institution of higher education, as defined by Section 61.003, Education Code;

(9) a volunteer fire department, as defined by Section 152.001, Tax Code; [~~and~~]

(10) an independent organization certified under Section 39.151, Utilities Code, for the ERCOT power region; and

(11) a retail public utility, as defined by Section 13.002, Water Code.

SECTION 3. Chapter 13, Water Code, is amended by adding Subchapter O to read as follows:

SUBCHAPTER O. CYBERSECURITY REQUIREMENTS

Sec. 13.601. DEFINITIONS. In this subchapter:

(1) "Center" means the Cyber Center for Security and Analytics at The University of Texas at San Antonio.

(2) "Department" means the Department of Information Resources.

Sec. 13.602. CONNECTION BETWEEN SUPERVISORY CONTROL AND DATA ACQUISITION SYSTEM AND INTERNET PROHIBITED. (a) A retail public utility may not connect the retail public utility's supervisory control and data acquisition system, or another equivalent operational information technology infrastructure, to the Internet.

(b) Notwithstanding Subsection (a), a supervisory control and data acquisition system or other equivalent operational information technology infrastructure may be operated by an intranet, site-to-site virtual private network.

(c) The commission, in consultation with the department, shall adopt rules as necessary to implement this section.

Sec. 13.603. REQUIREMENTS AND CONTROLS. (a) The commission, in consultation with and as recommended by the department and the center, by rule shall adopt cybersecurity requirements for retail public utilities to require the authentication of a retail public utility employee's identification before granting the employee access to a retail public utility's network or information systems.

(b) Not later than September 1 of each even-numbered year, the commission, in consultation with the department and the center, shall review and amend as necessary rules adopted under this section to ensure that the cybersecurity requirements continue to provide effective cybersecurity protection for retail public utilities.

Sec. 13.604. TRAINING. At least annually, a retail public utility shall:

(1) identify any employees and officials who:

(A) have access to the retail public utility's computer system or databases; or

(B) use a computer to perform any of the employee's or official's required duties; and

(2) require the employees and officials identified

under Subdivision (1) to complete a cybersecurity training program certified under Section 2054.519, Government Code.

Sec. 13.605. SECURITY ASSESSMENT AND COMPLIANCE AUDIT. (a) The commission, the utility commission, or the department may require a retail public utility to conduct, in accordance with commission and department rules:

(1) a security assessment of the retail public utility's:

(A) information resource systems;

(B) network systems;

(C) digital data storage systems;

(D) digital data security measures; or

(E) information resources vulnerabilities; or

(2) an audit of the retail public utility's compliance with this subchapter.

(b) Not later than the 90th day after the date a retail public utility completes a security assessment or audit under Subsection (a), the retail public utility shall report the results of the assessment or audit to:

(1) the commission;

(2) the utility commission; and

(3) the department.

(c) A standing committee of the legislature with jurisdiction over cybersecurity or water service may request that the commission, the utility commission, or the department require an assessment or audit under Subsection (a) from a retail public utility.

(d) The department shall provide to the center, and if applicable the standing committee of the legislature that requested the assessment or audit, access to each assessment or audit conducted under Subsection (a).

(e) The department or the center may conduct a security assessment or audit required by this section on behalf of a retail public utility.

(f) A retail public utility may contract with a person who is not the department or the center to conduct a security assessment or audit under this section.

(g) Information contained in a report prepared under this section is confidential and not subject to disclosure under Chapter 552, Government Code.

(h) The commission, in consultation with the department and the center, shall adopt rules as necessary to implement this section.

Sec. 13.606. SECURITY INCIDENT NOTIFICATION. (a) In this section:

(1) "Confidential information" means information the disclosure of which is regulated by law.

(2) "Sensitive personal information" has the meaning assigned by Section 521.002(a)(2)(A), Business & Commerce Code.

(b) A retail public utility that owns, licenses, or maintains computerized data that includes sensitive personal information or other confidential information shall notify the commission, the utility commission, the department, and the center of a security incident, not later than 48 hours after the discovery

of the incident, during which:

(1) a person other than the retail public utility made an unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information or other confidential information maintained by the retail public utility, including data that is encrypted if the person who acquired the data has the key required to decrypt the data;

(2) ransomware, as defined by Section 33.023, Penal Code, was introduced into a computer, computer network, or computer system; or

(3) unauthorized access of a computer information system or network led to a substantial loss of availability of the system or network or otherwise disrupted a retail public utility's ability to engage in business or deliver services.

(c) Subsection (b)(1) does not apply to a good faith acquisition of data by an employee or agent of the retail public utility for the purposes of the retail public utility if the employee or agent does not use or disclose the data in an unauthorized manner.

SECTION 4. Not later than September 1, 2026, the Texas Commission on Environmental Quality and the Department of Information Resources shall adopt the rules necessary to implement the changes in law made by this Act.

SECTION 5. A retail public utility shall comply with Section 13.602, Water Code, as added by this Act, not later than September 1, 2027.

SECTION 6. This Act takes effect September 1, 2025.