

By: Sparks, Perry

S.B. No. 1034

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

1 Section 5.001, Education Code;

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

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

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

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

10 (14) a governmental entity of another state; and

11 (15) a retail public utility, as defined by Section
12 13.002, Water Code.

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

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

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

22 (2) a local government;

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

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

- 1 (5) the Texas Permanent School Fund Corporation;
- 2 (6) an open-enrollment charter school, as defined by
- 3 Section 5.001, Education Code;
- 4 (7) a private school, as defined by Section 5.001,
- 5 Education Code;
- 6 (8) a private or independent institution of higher
- 7 education, as defined by Section 61.003, Education Code;
- 8 (9) a volunteer fire department, as defined by Section
- 9 152.001, Tax Code; ~~and~~
- 10 (10) an independent organization certified under
- 11 Section 39.151, Utilities Code, for the ERCOT power region; and
- 12 (11) a retail public utility, as defined by Section
- 13 13.002, Water Code.

14 SECTION 3. Chapter 13, Water Code, is amended by adding

15 Subchapter O to read as follows:

16 SUBCHAPTER O. CYBERSECURITY REQUIREMENTS

17 Sec. 13.601. DEFINITIONS. In this subchapter:

18 (1) "Center" means the Cyber Center for Security and

19 Analytics at The University of Texas at San Antonio.

20 (2) "Department" means the Department of Information

21 Resources.

22 Sec. 13.602. CONNECTION BETWEEN SUPERVISORY CONTROL AND

23 DATA ACQUISITION SYSTEM AND INTERNET PROHIBITED. (a) A retail

24 public utility may not connect the retail public utility's

25 supervisory control and data acquisition system, or another

26 equivalent operational information technology infrastructure, to

27 the Internet.

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

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

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

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

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

22 (1) identify any employees and officials who:

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

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

27 (2) require the employees and officials identified

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

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

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

9 (A) information resource systems;

10 (B) network systems;

11 (C) digital data storage systems;

12 (D) digital data security measures; or

13 (E) information resources vulnerabilities; or

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

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

20 (1) the commission;

21 (2) the utility commission; and

22 (3) the department.

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

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

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

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

11 (g) Information contained in a report prepared under this
12 section is confidential and not subject to disclosure under Chapter
13 552, Government Code.

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

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

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

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

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

1 of the incident, during which:

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

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

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

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

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

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

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