Texas Public
POLICY FOUNDATION
BETTER TECH FOR TOMORROW

BILL ANALYSIS: SENATE BILL 1034

PURPOSE

Senate Bill 1034 amends Section 2054.0525, Government Code, adding subsection 15 to classify retail public utilities as an eligible entity for participation in services provided by the Department of Information Resources (DIR). The bill also amends Section 2059.058, Government Code, adding subsection 11 to include retail public utilities as an entity eligible to receive network security services from DIR. Substantively, the bill amends Chapter 13, Water Code by adding Subchapter O which establishes cybersecurity requirements for retail public utilities, new definitions, cybersecurity training, security assessments and audits, and security incident notifications.

Retail public utilities1 have experienced a dramatic uptick in cyber incidents. Consider the following:

- In early 2024, hackers infiltrated multiple water and wastewater plants in West Texas, with subsequently leaked videos demonstrating hackers altering Supervisory Control and Data Acquisition (SCADA) systems remotely (James, 2024). For example, the city of Muleshoe, Texas, had a water tank overflow due to the cyberattack.

- Between January 2023 and January 2024, critical infrastructure systems throughout the world were attacked more than 420 million times, with attacks ranging in magnitudes. This equated to 13 attacks every second, a 30% increase from 2022 (KnowBe4, 2024).

- Due to the sensitivity of cybersecurity breach data, granular assessments on the number of water system attacks in Texas relative to other states are unavailable. However, Texas reported the second largest loss to cybercrime of all states in 2023 ($1.02 billion) and has the most reported cyber infiltrations of its water sector of any state (FBI, n.d.; DNI, 2024).

- An EPA assessment covering 1,062 drinking water systems for cybersecurity vulnerabilities identified 97 drinking water systems serving approximately 26.6 million users as having either critical or high-risk cybersecurity vulnerabilities (EPA, 2024a).

- Moreover, another inspection revealed that more than 70% of inspected water systems do not comply with cybersecurity requirements in the Safe Drinking Water Act (EPA, 2024b).

- 60% of critical infrastructure (CI) cyberattacks come from state-affiliated actors, namely China, Iran, Russia, and North Korea (Security Magazine, 2023)

Unfortunately, the lack of accurate data and reporting for cyberattacks on water systems renders an opaque picture of the state of cyber vulnerabilities in our water system. For example, after the FBI infiltrated known People's Republic of China cyberterrorist group Volt Typhoon's operations, they learned that the vast majority of victims never reported to the authorities that they were attacked. The real scale of damage is almost certainly much higher, potentially contributing to the lack of urgency for substantive legislative reform

SCADA systems are a hotbed for cyberattacks in the water sector. As noted by the Department of Energy,

- By allowing the collection and analysis of data and control of equipment such as pumps and valves from remote locations, SCADA networks provide great efficiency and are widely used. However, they also present a security risk. SCADA networks were initially designed to maximize functionality, with little attention paid to security. As a result, performance, reliability, flexibility and safety of distributed control/SCADA systems are robust, while the security of these systems is often weak. (n.d., p. 2)

In a May 2024 letter sent by the White House to all state governors, a plea for policy action was issued. Specifically, the letter states:

- Drinking water and wastewater systems are an attractive target for cyberattacks because they are a lifeline critical infrastructure sector but often lack the resources and technical capacity to adopt rigorous cybersecurity practices. … We need your support to ensure that all water systems in your state comprehensively assess their current cybersecurity practices to identify any significant vulnerabilities, deploy practices and controls to reduce cybersecurity risks where needed, and exercise plans to prepare for, respond to, and recover from a cyber incident. (Letter from Michael Regan and Jake Sullivan to state governors, 2024, pp. 1-2)

Section-by-Section analysis

Section 1

Amends Section 2054.0525, Government Code, adding retail public utilities (as defined by Section 13.002, Water Code) as an eligible customer for services from DIR.

Section 2

Amends Section 2059.058, Government Code, adding retail public utilities (as defined by Section 13.002, Water Code) as an entity eligible for the provision of network security services from DIR if the department agrees.

Section 3

Amends Chapter 13, Water Code, adding Subchapter O.

Section 13.601 provides new definitions, including "Center," meaning the Cyber Center for Security and Analytics at The University of Texas at San Antonio, and "Department," in reference to DIR.

Section 13.602 prohibits retail public utilities from connecting their SCADA system (or another equivalent operational information technology infrastructure) to the Internet. These systems can be operated by an intranet, site-to-site virtual private network (VPN), and the Texas Commission on Environmental Quality (the commission) shall consult with DIR to adopt rules as necessary for implementation.

Section 13.603 tasks the commission—upon consultation with DIR and the Center—to adopt by rule requirements for the authentication of a retail public utility employee's identification before they are granted access to the network or information systems. The commission is to work with DIR and the Center to review and amend adopted rules by September 1 of each even-numbered year to ensure that cybersecurity requirements are effective.

Section 13.604 requires retail public utilities to, at least annually, identify retail public utility employees who access or use computer systems or databases in their role, and require them to complete a cybersecurity training program certified under Section 2054.519, Government Code.

Section 13.605 stipulates that the commission, Public Utility Commission, or DIR may require a retail public utility to conduct a security assessment of the utility's information and digital system or an audit of their compliance with this subchapter. Within 90 days of conducting either requirement, the retail public utility shall report the results to all three aforementioned entities. Legislative committees with jurisdiction over cybersecurity or water may request that these three entities require such assessments of utilities. DIR or the Center may conduct these assessments on behalf of the utility, and utilities may contract with a separate individual to fulfill these requirements. Information contained in these reports is considered confidential and not subject to disclosure pursuant to Chapter 552, Government Code. The commission shall adopt rules as necessary, in consultation with DIR and the Center.

Section 13.606 defines “confidential information” and “sensitive personal information” (as defined by Section 521.002(a)(2)(A), Business & Commerce Code). Not later than 48 hours after the discovery of a security incident, the retail public utility shall notify the commission, Public Utility Commission, DIR, and the Center. This applies to security incidents where outside bad faith actors acquire data compromising sensitive or confidential information, ransomware, and unauthorized access resulting in system or network losses or a disruption in the ability to conduct business.

Section 4
Stipulates that the Commission and DIR shall adopt rules necessary to implement changes in the law no later than September 1, 2026.

Section 5
Stipulates that retail public utilities shall comply with the newly created Section 13.602, Water Code no later than September 1, 2027.

Section 6
Establishes an effective date of September 1, 2025.

References

Department of Energy (DOE). (n.d.). *21 steps to improve cyber security of SCADA networks*. Retrieved March 2, 2025, from https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

Environmental Protection Agency (EPA). (2024a, November 13). *Management implication report: Cybersecurity concerns related to drinking water systems*. https://www.epaoig.gov/sites/default/files/reports/2024-11/full_report_-_25-n-0004t_1.pdf

Federal Bureau of Investigation (FBI). (n.d.). *Federal Bureau of Investigation internet crime report 2023*. Retrieved March 4, 2025, from https://www.ic3.gov/annualreport/reports/2023_ic3report.pdf

James. (2024, October 13). *11 recent cyber attacks on the water and wastewater sector*. Wisdiam. https://wisdiam.com/publications/recent-cyber-attacks-water-wastewater/

KnowBe4. (2024). *Cyber attacks on infrastructure*: *The new geopolitical weapon*. https://www.knowbe4.com/hubfs/Global-Infrastructure-Report-2024_EN_US.pdf

Letter from Michael Regan and Jake Sullivan to state governors. (2024, March 18). Environmental Protection Agency. https://www.epa.gov/system/files/documents/2024-03/epa-apnsa-letter-to-governors_03182024.pdf

Office of the Director of National Intelligence (DNI). (2024). *Recent cyber attacks on US infrastructure underscore vulnerability of critical US Systems, November 2023–April 2024*. https://www.dni.gov/files/CTIIC/documents/products/Recent_Cyber_Attacks_on_US_Infrastructure_Underscore_Vulnerability_of_Critical_US_Systems-June2024.pdf

Security Magazine. (2023, September 19). *Energy sector faces 39% of critical infrastructure attacks*. https://www.securitymagazine.com/articles/99915-energy-sector-faces-39-of-critical-infrastructure-attacks