



Protecting Your Utility!

TCEQ Requirements

Required Incident Reporting and Assistance

Per existing TCEQ rule water systems must report cybersecurity incidents to the TCEQ immediately, *Title 30 Texas Administrative Code, Chapter 290, Subchapter D, §290.46(w), Security*:

§290.46(w) Security. All systems shall maintain internal procedures to notify the executive director by a toll-free reporting phone number immediately of the following events, if the event may negatively impact the production or delivery of safe and adequate drinking water:

§290.46(w)(1) an unusual or unexplained unauthorized entry at property of the public water system;

§290.46(w)(2) an act of terrorism against the public water system;

TCEQ Requirements (2)

Required Incident Reporting and Assistance Continued:

§290.46(w)(3) an unauthorized attempt to probe for or gain access to proprietary information that supports the key activities of the public water system;

§290.46(w)(4) a theft of property that supports the key activities of the public water system; or

§290.46(w)(5) a natural disaster, accident, or act that results in damage to the public water system.

TCEQ Resources

The cybersecurity information is located on the TCEQ public drinking water page under:

Homeland Security for PWS

Cybersecurity resources can be found at the following websites:



State Resources and Requirements

- [Texas Department of Information Resources \(DIR\)](#) 
- [Texas Department of Information Resources Cybersecurity Incident Management and Reporting](#) 
 - As of September 1, 2023, local governments are required to report security incidents to DIR, within 48 hours of discovery. This includes non-profit water systems that include municipalities, counties, districts, and water authorities.
- [Texas Attorney General Data Breach Reporting](#) 
 - As of September 1, 2023, Texas law requires businesses and organizations that experience a data breach of system security affecting 250 or more Texans to report that breach to the Office of the Texas Attorney General no later than 30 days after discovery of the breach.

Federal Resources

- [Cybersecurity & Infrastructure Security Agency \(CISA\)](#) 
 - CISA helps critical infrastructure owners and operators understand the importance of their facility, how their service fits into a critical infrastructure sector, and the CISA resources available to enhance their security and resilience. This agency can assist for-profit water systems with cybersecurity issues.
- [CISA Water and Wastewater Cybersecurity](#) 
- [CISA Critical Infrastructure Water Sector](#) 
-  [CISA Incident Response Guide](#) 
-  [CISA Fact Sheet: Top Cyber Actions for Securing Water Systems](#) 
- [EPA Cybersecurity Best Practices for the Water Sector](#) 
- [FBI Cyber Crime Reporting](#) 

Other Resources

- [AWWA Resources on Cybersecurity](#) 
- [Water Information Sharing and Analysis Center \(WaterISAC\)](#) 

Any security breaches, either cyber or physical, should be reported to the TCEQ at PDWS@tceq.texas.gov.

What is Cybersecurity?

Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.

Almost everything relies on computers and the internet now:

- communication (e.g., email, smartphones, tablets)
- entertainment (e.g., interactive video games, social media, apps)
- transportation (e.g., navigation systems)
- shopping (e.g., online shopping, credit cards)
- medicine (e.g., medical equipment, medical records), and the list goes on.

How much of your personal information is stored either on your own computer, smartphone, tablet or on someone else's system?

State Requirements

Texas Department of Information Resources (DIR)

- As of September 1, 2023, local governments are required to report security incidents to the **Texas DIR**, within 48 hours of discovery.
- This includes non-profit water systems such as municipalities, counties, districts, water authorities and water supply corporations.

State Requirements ⁽²⁾

Office of the Texas Attorney General

As of September 1, 2023, Texas law requires businesses and organizations that experience a data breach of system security affecting 250 or more Texans to report that breach to the Office of the Texas Attorney General no later than 30 days after discovery of the breach.

<https://www.texasattorneygeneral.gov/consumer-protection/data-breach-reporting>

State Resources

Texas Department of Information Resources (DIR)

Texas DIR offers technology services to state and local government entities this includes:

- Providing organizations with incident response support, guidance, and resources, before, during, and after a cybersecurity incident.
- Improving cybersecurity across Texas using the Texas Information Sharing and Analysis Organization (TX-ISAO).

Federal Requirements

The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

- CIRCIA was signed into law by the President on March 2022, the act requires the Cybersecurity & Infrastructure Security Agency (CISA) to develop and implement regulations requiring critical infrastructure entities (water utilities) to report cyber incidents and ransomware payments to CISA.
- CISA will have to complete rulemaking activities before the reporting requirements go into effect.

Federal Resources

Cybersecurity & Infrastructure Security Agency (CISA)

- CISA helps critical infrastructure owners and operators understand the importance of their facility, how their service fits into a critical infrastructure sector, and the CISA resources available to enhance their security and resilience. This agency can also assist water systems with cybersecurity issues.
- Provides **free** Cyber Vulnerability Scanning for Water Utilities to identify vulnerabilities that adversaries could use to conduct a cyberattack.

Federal Requirements ⁽²⁾

Environmental Protection Agency (EPA)

America's Water Infrastructure Act of 2018 (AWIA)

Requires community (drinking) water systems (CWSs) serving more than 3,300 people to develop or update risk and resilience assessments (RRAs) and emergency response plans (ERPs). The law specifies the components that the RRAs and ERPs must address and establishes deadlines by which water systems must certify to EPA completion of the RRA and ERP.

AWIA Requirements

List of vulnerabilities required to be evaluated and utilized to create Emergency Response Plan.

Risk and Resilience Assessment (RRA)

RRAs evaluate the vulnerabilities, threats, and consequences from potential hazards. AWIA RRAs shall assess the risks to and resilience of specified assets to malevolent acts and natural hazards, including:

- physical barriers
- source water
- pipes and constructed conveyances, water collection and intake
- pretreatment and treatment
- storage and distribution facilities
- electronic, computer, or other automated systems (including the security of such systems)
- monitoring practices
- financial infrastructure
- the use, storage, or handling of chemicals
- operation and maintenance of the system

AWIA Requirements (2)

List of findings ERPs shall address:

- Strategies and resources to improve resilience, including physical and cybersecurity.
- Plans and procedures for responding to a natural hazard or malevolent act that threatens safe drinking water.
- Actions and equipment to lessen the impact of a malevolent act or natural hazard, including alternative water sources, relocating intakes and flood protection barriers.
- Strategies to detect malevolent acts or natural hazards that threaten the system.

AWIA Deadlines: RAA

- Every five years, the utilities must review the **RRA** and submit a recertification to the EPA that the assessment has been reviewed and, if necessary, revised.

Next 5-year cycle certification deadlines for **RRA**:

Population Served	Previous RRA Deadline	Next 5-Year Submission Cycle RRA Deadline
≥100,000	March 31, 2020	March 31, 2025
50,000-99,999	December 31, 2020	December 31, 2025
3,301-49,999	June 30, 2021	June 30, 2026

AWIA Deadlines: ERP

- Utilities must develop or update an **ERP** and certify completion to EPA no later than six months after RRA certification.

Next 5-year cycle certification for **ERP**:

Population Served	Previous ERP Deadline	Next 5-Year Submission Cycle ERP Deadline
≥100,000	September 30, 2020	September 30, 2025
50,000-99,999	June 30, 2021	June 30, 2026
3,301-49,999	December 31, 2021	December 31, 2026

Federal Resources ⁽²⁾

EPA is encouraging all water and wastewater utilities to employ cybersecurity best practices by providing water utilities with technical assistance via multiple tools such as the:

- Cybersecurity Evaluation and Technical Assistance Programs
- Cybersecurity Checklists
- Cybersecurity Planning for preparing, responding, and recovering from a cyber incident
- Cybersecurity Training and Funding
- Partnerships to support cybersecurity incident response

Additional Resources

- **American Water Works Association**
Cybersecurity Assessment Tool and Guidance

- **WaterISAC**

The U.S. water and wastewater sector's leading national associations and research foundations established the Water Information Sharing and Analysis Center (WaterISAC) in 2002, in coordination with the EPA.



Questions....

Leticia De Leon, Technical Specialist
Drinking Water Homeland Security Coordinator
Emergency Preparedness and Response Section
(512) 965-2371 or Leticia.deleon@tceq.texas.gov