TEXAS WATER UTILITIES
CYBER THREAT BRIEF

CoreRecon Intelligence Report | June 2026

SDVOSB Certified | 30-Min OT IR SLA | Texas-Based SOC

AWIA Section 2013 + EPA RY2 + CISA CPGs + TCEQ Compliance

CYBERARMY OF RUSSIA HIT 4 TX PANHANDLE WATER UTILITIES — MULESHOE TANK OVERFLOWED

Hale Center · Abernathy · Lockney | Unitronics Vision PLCs | VNC with no auth | Jan 2024 | CISA AA24-057A

AWIA §2013 mandates SCADA cybersecurity assessment | EPA RY2 | 7,000+ TX public water systems at risk

RECENT CONFIRMED OT INCIDENTS

Muleshoe, TX	**Tank overflow**	CyberArmyofRussia | Unitronics PLC | VNC no auth | manual shutdown	Jan 2024
Hale Center, TX	**OT compromise**	Same threat actor wave — same hardware, same default credentials	Jan 2024
North TX Mun. WD	**Data breach**	Daixin Team ransomware | 1.1M customer records exfiltrated	Nov 2023
Aliquippa PA	**PLC hijack**	CyberAv3ngers (IRGC-linked) | Unitronics PLC banner | "You've been hacked"	Nov 2023

APPLICABLE REGULATIONS

AWIA Section 2013 (SCADA mandatory) • EPA RY2 Risk & Resilience Assessment • CISA CPGs (Water Sector) • TCEQ §290 • TX SB 820 (48-hr breach notification)

FREE POSTURE ASSESSMENT — NO OBLIGATION

https://corerecon.polsia.app/assessment?industry=Water+Utilities | (800) 955-2596

John Martinez — Founder & CEO, CoreRecon. U.S. Marine Corps Veteran. SDVOSB Certified. AT&T Vendor for State of Texas Incident Response. Corpus Christi, TX.

SECTION 1 — TX WATER UTILITY THREAT LANDSCAPE

Texas has over 7,000 public water systems, the vast majority operated by municipalities and water districts with minimal IT staff. The January 2024 CyberArmyofRussia attack on four Panhandle utilities proved the threat is not theoretical — factory-default credentials on internet-accessible Unitronics PLCs created a direct path to physical impact. The Muleshoe tank overflow closed the argument that "it won't happen to a small utility."

THE MULESHOE INCIDENT — DEFINING THE RISK

- !’ January 2024: CyberArmyofRussia (Sandworm-linked hacktivist group) compromised HMIs at Muleshoe, Hale Center, Abernathy, and Lockney simultaneously
- ! Attack vector: Unitronics Vision PLCs with VNC enabled, no authentication, port 5900 exposed on public internet — findable on Shodan in seconds
- ! Muleshoe result: water tank overflowed before operators noticed and switched to manual control — a direct physical public health impact
- ! CISA Emergency Advisory AA24-057A (Feb 2024) documented the TTP and found the same hardware widely deployed across US water utilities

6 THREAT ACTORS TARGETING WATER SECTOR OT

CRITICAL	GRU-linked. TX Panhandle Jan 2024. VNC HMI access. Hacktivist front with nation-state capability and physical intent.
CRITICAL	Iran IRGC-affiliated. Aliquippa PA Nov 2023 — "You've been hacked" banner on Unitronics PLC. Same hardware as TX utilities.
HIGH	Ransomware + data extortion. North TX Municipal Water District (Nov 2023) — 1.1M customer records. Demand + public leak.
HIGH	Double-extortion. Healthcare + utilities. Documented SCADA lateral movement. Supply chain entry via IT network.
HIGH	Ransomware. Hit multiple critical infrastructure operators 2023-2024. Known for fast lateral movement from IT to OT.
HIGH	China MSS pre-positioning. CISA/FBI AA24-038B. TX water, energy, and telecom confirmed targets. Living-off-the-land persistence.

SECTION 2 — AWIA + REGULATORY COMPLIANCE STACK

The America's Water Infrastructure Act (AWIA) Section 2013 changed everything. Community water systems serving more than 3,300 people must complete a Risk and Resilience Assessment that explicitly names cybersecurity of SCADA, HMI, and industrial control systems. The compliance calendar is active — EPA has begun enforcement reviews. A ransomware event during an open RRA window compounds legal and federal funding exposure.

ENFORCEMENT ACTIVE

- %¸ Mandatory for all community water systems (CWSs) serving >3,300 people — covers cybersecurity of SCADA, HMI, and ICS as named requirement
- %¸ RRA must be submitted to EPA and updated every 5 years; Emergency Response Plan (ERP) updated within 6 months of RRA certification
- %¸ Cybersecurity scope (per EPA guidance): SCADA and control systems, data integrity, system backup and recovery, communications, monitoring
- %¸ AWIA §1433 grants: up to $125K per system for RRA and ERP development — funding available but requires documented cybersecurity posture

HIGH PRIORITY

- %¸ EPA's 2023 memorandum explicitly required states to audit water system cybersecurity during sanitary surveys
- %¸ Three-state lawsuit (MO, AR, IA) paused enforcement in 2023 — but EPA RY2 guidance remains in place and states continue audits
- %¸ CISA and EPA joint advisory (AA22-249A): water utilities remain high-value targets due to thin security posture and OT exposure
- %¸ Documented cybersecurity program is required evidence for federal infrastructure grants (IIJA, EPA WIFIA, SRF applications)

COMPLIANCE BASELINE

- %¸ CISA CPG 2.0 (August 2023): 17 goals directly applicable to water utilities — asset inventory, network segmentation, MFA, incident response
- %¸ CPG 1.A: Asset inventory required for all OT equipment including PLCs, HMIs, SCADA components — most TX systems lack complete inventories
- %¸ CPG 2.B: Privileged access management for ICS — vendor remote access MFA is a specific CPG requirement, directly addresses Muleshoe attack vector
- %¸ WaterISAC 15 Foundational Security Actions: aligned to CPGs and AWIA, used as baseline by EPA auditors

TX-SPECIFIC

- %¸ TCEQ Chapter 290 (Public Water Supply): operational continuity requirements — cyber incidents that compromise distribution trigger reporting
- %¸ TX SB 820 (eff. Sept 2023): state agency 48-hour breach notification mandate; municipalities using cloud billing systems are in scope
- %¸ TDPSA (eff. July 1, 2024): Texas Data Privacy and Security Act — water districts collecting customer data have new data handling obligations
- %¸ TX Cybersecurity Framework (DIR): applicable to political subdivisions including water districts and municipal utilities

SECTION 3 — OT/IT ATTACK SURFACE

Water utility SCADA environments combine decades-old industrial hardware with modern IP connectivity. Unitronics Vision series PLCs — the exact hardware in the Muleshoe attack — are deployed across hundreds of TX water systems. The attack surface is not complex: VNC enabled, port 5900 open, factory-default credentials, internet-facing. Shodan finds them in seconds. The Muleshoe operator switched to manual control. Most utilities won't catch it that fast.

Risk: CRITICAL

- Unitronics Vision series PLCs: factory-default VNC passwords documented in CISA ICS-CERT advisories since 2019 — still deployed in TX
- Port 5900 (VNC) / port 20256 (Unitronics native) on public IP: discoverable on Shodan with simple queries — no hacking required
- CISA ICS Advisory ICSA-23-320-05: Unitronics Vision series authentication bypass — CVSS 10.0 — vendor patch rate below 30%
- Beyond Unitronics: Schneider Electric Modicon, Rockwell Allen-Bradley, GE MDS radios — all with documented public CVEs affecting TX utilities

Risk: CRITICAL

- Modbus TCP: no native authentication or encryption — transmits pump commands and sensor readings in plaintext on most TX SCADA networks
- DNP3 without Secure Authentication v5 (SAv5): susceptible to replay attacks, man-in-the-middle, and command injection — SAv5 adoption under 20%
- Most IT security tools cannot parse Modbus/DNP3 — standard SIEM generates no alerts for anomalous industrial protocol traffic
- Active scanning can crash PLCs — passive OT protocol monitoring is required; active scanning is disqualifying in a water utility environment

Risk: HIGH

- Operators use Windows desktops in the control room that also access corporate email — direct IT/OT bridge without intentional design
- Vendor remote access: water treatment chemical vendors, SCADA integrators, and telemetry providers often retain persistent VPN access
- Cellular modems on pump stations and lift stations: "management" SIM cards with no authentication relay Modbus commands to field PLCs
- COVID-era remote operation: many TX utilities expanded remote access in 2020 without security review — many configurations never tightened

Risk: HIGH

- North TX Municipal Water District (Nov 2023): Daixin ransomware exfiltrated billing/customer data via IT network, not OT — 1.1M records
- CIS (Customer Information System) and billing platforms share infrastructure with corporate IT — ransomware hits both simultaneously
- AMR/AMI meter data flows from field to billing system through corporate network — creates lateral movement path from billing to SCADA historian
- SCADA historian databases accessible from the same Windows network as email: historian data feeds are often unsegmented

SECTION 4 — CONFIRMED INCIDENT CASE STUDIES

Every case below is a documented public incident with attributed threat actors and verified impact. These are not theoretical scenarios — they are precedents that directly apply to Texas water and wastewater utilities. The AWIA RRA process requires documented threat actor analysis; this section provides that analysis with sources.

CRITICAL January 2024

- CyberArmyofRussia (Sandworm-linked) accessed Unitronics Vision PLC/HMI via VNC with factory-default credentials
- Attacker manipulated controls to raise water level in a holding tank — tank overflowed before operator noticed
- No remote monitoring, no SOC, no alert system — physical operators identified the overflow manually
- Simultaneously hit Hale Center, Abernathy, and Lockney — same hardware, same credentials, same vector
- CISA Emergency Advisory AA24-057A: verified incident, specific TTPs documented, nationwide exposure confirmed

CRITICAL November 2023

- Daixin Team ransomware attack — not OT-targeted but IT network fully compromised
- 1.1 million customer records exfiltrated: names, addresses, SSNs, banking information for water bill autopay
- SCADA operations not directly impacted — but IT paralysis created indirect operational disruption
- TX SB 820 notification obligations triggered — 48-hour notice to state AG office required
- Lesson: billing and IT network compromise creates customer data liability and operational disruption without touching OT

CRITICAL November 2023

- CyberAv3ngers (Iran IRGC Cyber Command-affiliated) targeted Unitronics PLC/HMI — same exact hardware as TX Panhandle
- Displayed "You have been hacked" banner on operator HMI screen — attacker had full control of displayed interface
- Booster station taken offline — backup manual controls activated, water pressure maintained
- CISA ICS Alert AA23-335A confirmed the incident — specifically warned of ongoing Unitronics targeting nationwide
- IRGC-linked actors openly boasting of water system access: a deliberate psychological operation against US public utilities

HIGH February 2021

- Attacker used TeamViewer to access SCADA — operator watched mouse move and controls change in real-time
- Sodium hydroxide (lye) concentration increased to 111x normal level — operator manually reversed within minutes
- No credential theft, no malware — legitimate remote access tool with shared or default credentials
- Wake-up call: OT remote access without MFA, session logging, or access review creates direct poisoning pathway
- Direct parallel to every TX water utility running TeamViewer, AnyDesk, or VNC without enhanced authentication

SECTION 5 — INCIDENT RESPONSE REALITY & COMPETITOR LANDSCAPE

Most Texas water utilities operate with zero dedicated cybersecurity staff. An OT incident at 2am Saturday has no escalation path to a cybersecurity professional within an hour — unless a managed service is in place. The WaterISAC and CISA offer guidance, but neither provides a managed SOC or 24/7 incident response. The Muleshoe operator caught the overflow because they physically saw it. Most attacks won't be that visible.

MUTUAL AID & FREE PROGRAM LIMITATIONS

- !’ WaterISAC: threat intelligence sharing hub — excellent for awareness, not a managed SOC or incident response service
- !’ CISA Region 6 (TX): available for guidance and post-incident support — does not provide 24/7 real-time monitoring
- !’ AWWA Cybersecurity Guidance: WaterTrust and Operational Technology Cybersecurity Initiative — frameworks, not managed coverage
- !’ EPA WaterCISA Cybersecurity for Water Utilities: resources and training — not a SOC or IR retainer
- !’ None of the above provide a 30-minute response SLA for an active OT incident on a Saturday night

COMPETITOR LANDSCAPE

FREE for small utilities	OT threat intel platform — no managed service. Useful baseline, but platform knowledge doesn't equal 24/7 SOC coverage or IR response. CoreRecon fills the managed layer Dragos does not provide.
Enterprise pricing	Broad OT asset visibility — engineering-heavy deployment, 90+ day implementation, enterprise deal sizes above water district budgets. No SOC included.
IT-first MDR	No native Modbus/DNP3 understanding. Effective against ransomware on IT networks but cannot detect OT-specific protocol anomalies. Leaves OT network uncovered.
Current state	Most TX water utilities: 0-1 IT staff, no cybersecurity background, business hours only. Zero OT protocol knowledge. CoreRecon Command tier augments without requiring headcount.

8 CONTROLS EVERY TX WATER UTILITY NEEDS IN 2026

01

Change factory-default passwords on every Unitronics, Allen-Bradley, Schneider Electric, and GE PLC immediately. The Muleshoe attack vector was a documented default VNC password from 2014. CISA has published default credentials for over 40 water-sector ICS vendors. This is the highest-priority single action.

02

VNC, RDP, and vendor-specific management ports (Unitronics 20256, Modbus 502, DNP3 20000) must not be exposed to the internet. Firewall audit required immediately. All remote access must flow through VPN or jump server — never direct internet exposure.

03

MFA required on all VPN, remote desktop, vendor support sessions, and SCADA historian access. The Oldsmar FL attack (2021) used TeamViewer with shared credentials — no MFA. AWIA and CISA CPG 2.B both require privileged access management with MFA for ICS environments.

04

SCADA/ICS network must be isolated from the corporate LAN that handles email, billing, and administrative systems. A ransomware attack on billing (North TX MWD model) must not have lateral movement path to SCADA. Documented network segmentation is required in AWIA RRA cybersecurity section.

05

Deploy passive network monitoring that understands Modbus and DNP3 without sending packets that crash PLCs. Active scanning is contraindicated — passive monitoring detects anomalous command sequences and new device connections. CoreRecon Fortress includes OT protocol monitoring supplement.

06

WORM-compliant backup of billing/CIS, SCADA historian, and PLC configuration files. Air-gapped or offsite copy. Tested recovery — not just backup existence. North TX MWD was offline for weeks; DMEA CO was offline 1+ month. A tested recovery plan is the difference between days and months.

07

Written IR plan aligned to AWIA Emergency Response Plan requirements and CISA CPG 5.A. Maps escalation to CISA Region 6, WaterISAC, and EPA. Includes 24/7 contact for a cybersecurity professional — not just the IT director's cell phone. Table-top test annually.

08

Document every PLC, HMI, RTU, flow meter transmitter, and SCADA component — including firmware version and network address. AWIA RRA requires cybersecurity scope defined by asset inventory. Most TX utilities cannot pass an EPA audit without a current OT asset inventory; most don't have one.

30 / 60 / 90 DAY ROADMAP

Days 1–30 — Close the Open Doors

- !’ Audit all PLCs/HMIs for factory-default credentials — Unitronics, Allen-Bradley, Schneider Electric, GE
- !’ Remove all internet-facing VNC, RDP, Modbus, and DNP3 ports — verify with external port scanner
- !’ Enable MFA on all VPN and remote access paths — vendor sessions, operator remote access, historian access
- !’ Conduct OT asset inventory: PLC, HMI, RTU, telemetry, SCADA components — firmware versions included

Days 31–60 — Harden the Environment

- !’ Segment SCADA/ICS network from corporate IT LAN — verify no flat network paths from email/billing to PLCs
- !’ Deploy passive OT protocol monitoring for Modbus and DNP3 anomaly detection
- !’ Test backup recovery for billing/CIS system — document RTO; test SCADA historian restore
- !’ Draft AWIA-compliant Emergency Response Plan — align to CISA Region 6 escalation path

Days 61–90 — Operational Resilience

- !’ Table-top incident response exercise: ransomware-on-Saturday-night + OT network compromise scenario
- !’ Complete AWIA Risk & Resilience Assessment cybersecurity section using asset inventory and controls documentation
- !’ Submit/update RRA to EPA — preserve evidence of cybersecurity program maturity for federal grant applications
- !’ Brief utility board and city council on cyber risk posture, Muleshoe precedent, and 30-min SLA value

CORERECON PRICING FOR TX WATER UTILITIES & DISTRICTS

SENTINEL

$89/endpoint/mo

- 24/7 MDR (Managed Detection & Response)
- EDR + SIEM + threat hunting
- AWIA RRA evidence documentation
- Breach notification workflow support
- Best for: small districts, <50 endpoints

20 endpoints = $1,780/mo

FORTRESS

$109/endpoint/mo

- Everything in Sentinel
- 30-min OT IR SLA (live TX SOC)
- OT protocol monitoring (Modbus/DNP3)
- AWIA + CISA CPG Compliance Pack
- Best for: mid-size utilities, SCADA environments

30 endpoints = $3,270/mo

COMMAND

$129/endpoint/mo

- Everything in Fortress
- vCISO + co-managed security model
- AWIA RRA and ERP documentation support
- Annual tabletop exercise included
- Best for: large districts, multiple plant sites

50 endpoints = $6,450/mo

vs. Claroty/Forescout: enterprise pricing • vs. Dragos: platform only, no managed SOC • vs. Arctic Wolf: IT-first, no OT protocol coverage

SDVOSB status: federal grant applications requiring demonstrated cybersecurity program include CoreRecon as verified vendor — advantage no IT MSSP can replicate.

FREE POSTURE ASSESSMENT — NO OBLIGATION

30-minute call. We map your OT/IT environment, PLC exposure, and AWIA RRA gaps.

https://corerecon.polsia.app/assessment?industry=Water+Utilities • (800) 955-2596

John Martinez — Founder & CEO, CoreRecon

U.S. Marine Corps Veteran. SDVOSB Certified. AT&T Vendor for State of Texas Incident Response. Corpus Christi, TX.
CoreRecon delivers 24/7 OT-aware SOC for Texas water utilities at $89–$129/endpoint — with AWIA, CISA CPG, and Modbus/DNP3 protocol expertise no national MSSP can match.