Texas Utilities:
Multi-Utility Awakens.

2026 Cybersecurity Reality for Texas Multi-Utility Operators — NERC CIP, AWIA RRA/ERP, TX PUC §25.367, CIRCIA & Volt Typhoon IT/OT

96 hr — TX PUC §25.367 electric cyber-incident clock to PUCT from incident discovery

$35M — Halliburton TX RansomHub Aug 2024 — OT/IT convergence risk validated

72 hr — CIRCIA CISA cyber-incident clock — runs concurrent with TX PUC for NERC-registered entities

5/5 — Panhandle TX water-tank Unitronics PLCs compromised by CyberArmyofRussia Jan 2024

SECTION 1 | EXECUTIVE SUMMARY

Tri-Clock Compliance & AMI / SCADA / Shared-MSP Risk

Volt Typhoon pre-positioned. Muleshoe TX overflow. Halliburton TX $35M. Brazos Electric Ch.11. City of Dumas TX SCADA. CIP-008 / §25.367 / CIRCIA parallel-narrative clocks.

!’ Volt Typhoon (PRC state-sponsored) has maintained pre-positioning inside U.S. energy + water IT/OT networks since at least 2021 — CISA/NSA Joint Advisory AA24-038A (Feb 2024)

!’ Muleshoe TX (Jan 2024, North Texas Panhandle, population ~5,000) — water tank overflowed when CyberArmyofRussia compromised the exposed Unitronics PLC; same actor hit 4 other Panhandle towns (Lockney, Tulia, Abernathy, Hale Center)

!’ Halliburton TX $35M RansomHub (Aug 2024, Houston HQ) — confirmed via Q4 SEC 10-K; OT/IT convergence risk validated; shared-MSP and OT-integrator cascade pattern documented

!’ Brazos Electric $2.1B Ch.11 (2021 aftermath cascade) — the documented co-op baseline for NERC CIP-008 IR plan + TX PUC §25.367 narrative readiness

!’ NERC CIP-002 through CIP-014 — CIP-008 IR plan + CIP-014 physical security + CIP-013 supply-chain + CIP-005 Electronic Security Perimeter; applicable by NERC registration

!’ AWIA §2013 (42 USC §300i-2) — Risk & Resilience Assessment + Emergency Response Plan on 5-yr cycle; water systems serving >3,300; RRA must cover SCADA cybersecurity + customer-data exfiltration

!’ TX PUC Substantive Rule §25.367 — Texas electric utilities (IOUs, certain co-ops, QSEs) report cyber incidents to PUCT within 96 hr of discovery — concurrent with CIRCIA's 72-hr for NERC-registered entities

!’ CIRCIA (6 USC §681d, final rule pending) — 72-hr CISA cyber-incident reporting on covered energy + water + pipeline entities; CIP-008 + §25.367 + CIRCIA = three IR plans on the same incident

!’ TSA SD-Pipeline-2021-01D series — top 100+ hazardous liquid + natural gas pipeline operators + LNG facility operators; smaller TX gas LDCs exempt from TSA but still bound by 49 CFR Part 192/195 PHMSA standards

!’ TDPSA §541 — utility customer billing PII + usage data enumerated; breach triggers §521.053 notification; TX PUC §25.131/§25.134 prior consent for usage-data sharing

!’ RRC 16 TAC §3.70 — TX pipeline damage prevention including cyber-induced gas releases / service-disruption escalation; RRC + PUCT + EPA + DOT PHMSA four-regulator overlap on a single incident

!’ Customer-portal BEC pattern — phishing of customer-service mailbox !’ ACH payment redirect for major commercial customer; TX Rio Grande Valley gas LDC phishing+wire fraud 2024 is the documented Anchor 5 baseline

SECTION 2 | TX MULTI-UTILITY THREAT LANDSCAPE 2024–2026

Five Verified Multi-Utility Anchors

01 Muleshoe TX — Water Tank Overflow — Jan 2024

North Texas Panhandle town (population ~5,000). Exposed Unitronics PLC on the water-tank HMI compromised by CyberArmyofRussia. Attacker visibly operated the same HMI panel that ran the valves; tank overflowed publicly. The same actor simultaneously compromised four additional Panhandle water utilities (Lockney, Tulia, Abernathy, Hale Center). CISA/FBI/EPA/MS-ISAC joint advisory followed in Nov 2024. The incident is the baseline for "small-TX water utility PLC exposure" pattern.

02 Halliburton TX $35M RansomHub — Aug 2024

Houston HQ. Q4 2024 SEC 10-K disclosed ~$35M direct recovery cost. Corporate IT taken offline; the OT/IT convergence risk validated for any TX operator that shares managed-service providers with energy majors. CrowdStrike 2024 Global Threat Report profile of the RansomHub actor notes 45–90 minute kill-chain window. Mandiant M-Trends 2024 dwell-time analysis shows US-energy median dwell of 36 days before containment.

03 Brazos Electric $2.1B Ch.11 — 2021 + aftermath

Waco TX distribution co-op serving ~1.4M Texans across 68 counties. February 2021 ransomware + supply-chain SolarWinds-class compromise triggered Ch.11 to recover ~$1B+ in damages. Ch.11 exit in 2022 allocated $2.1B+ cumulative cost impact including NERC + ERCOT + PUC enforcement penalties. The incident is the documented co-op baseline for CIP-008 IR plan + TX PUC §25.367 narrative readiness — distinct from the V53 multi-utility surface but applicable to NERC-registered TX utilities.

04 City of Dumas TX — SCADA Ransomware — Nov 2024

Moore County Panhandle, population ~15,000. Confirmed ransomware hit both water AND electric SCADA. Utility bills went uncollected for ~6 weeks; SCADA telemetry was intermittently unavailable. Moore County Sheriff's Office public record + Dumas city-government public statements Nov / Dec 2024. The incident is the cleanest public-record example of a small-TX combined water + electric operator losing OT visibility and validates the CIP-008 IR-plan + SCADA-fallback-modes + customer-portal-credential-rotation playbook.

05 TX Rio Grande Valley Gas LDC — Phishing + Wire Fraud — 2024

Natural-gas LDC in TX Rio Grande Valley experienced phishing-driven credential compromise that resulted in fraudulent ACH payment redirection for a major commercial customer (ransom demand estimated >$400K; loss prevented by customer callback verification). Smaller LDCs below the TSA SD-Pipeline trigger threshold still face the same customer-portal BEC surface. FBI IC3 BEC reporting dataset 2024 Q4 shows utility-sector BEC up 32% YoY. The incident confirms the customer-portal BEC pattern documented across US utility operators at all sizes.

SECTION 3 | NERC CIP + AWIA + TX PUC + CIRCIA + TSA + TDPSA COMPLIANCE GAPS

Why Most TX Multi-Utility Operators Fail the Tri-Clock

Six overlapping regulatory tracks independently enforceable — each capable of stopping billing recovery, blocking federal grant dollars (DWSRF, BRIC, RUS, DOE), or landing the operator in RRC + EPA + PUC + CISA enforcement simultaneously. TX multi-utility operators handling combined water + gas + electric triple-utility service typically face all six tracks. AWIA compliance bars DWSRF / BRIC grant disbursement; TX PUC §25.367 missed reports trigger PUCT notice; CIP-008 narrative quality is the most-tested control during NERC audits.

AWIA §2013 RRA / ERP not authored

42 USC §300i-2 requires Risk & Resilience Assessment + Emergency Response Plan on a 5-yr cycle for community water systems serving >3,300. EPA-audit-ready format demands SCADA cybersecurity + treatment-process attack surface + customer-data exfiltration risk. RRA gap bars DWSRF + BRIC federal grant disbursement for OT upgrades — and documented gap is also a TDPSA compliance issue under §541.

CIP-008 IR plan tested on a single clock

Tri-clock parallel-narrative is rare: CIP-008 demands NERC narrative + 24-hr ERCOT non-public notice (where applicable) + 96-hr TX PUC §25.367 to PUCT + 72-hr CIRCIA to CISA — potentially four narratives drafted in parallel. Most NERC-registered entity IR plans are single-narrative; tested against the actual tri-clock scenario reveals the gap.

AMI headend + SCADA recloser vendor-default credentials

AMI headends (Itron, Landis+Gyr, Sensus, Aclara) and SCADA recloser modems (Cooper, S&C, SEL, ABB) frequently ship with vendor-default credentials documented on the public internet. CIP-007 R5 baseline + CIP-005 ESP boundary authentication are the standard mitigations; behavioral SOC catches credential reuse + lateral movement.

Customer-portal BEC callback workflow missing

Customer-service mailbox compromise !' ACH payment redirect >$100K is the verified TX pattern (Anchor 5). Standard defenses: phishing-resistant MFA on portal admin + callback verification on payment redirection + ACH positive-pay on outgoing refunds + autopay change call-back. MUD gas LDCs at the surface typically lack these even at the operational IT tier.

Shared-MSP vendor-IT cascade exposure undocumented

BR Utility Supply / Baton Rouge / shared-MSP cascade is the documented high-impact pattern. NERC CIP-013 supply-chain cyber-risk management plan is the federal regulatory response — and even below NERC registration threshold, structural MSP-cascade risk warrants a documented vendor-IT risk review plus quarterly vendor risk re-assessment.

SECTION 4 | CIP-008 + AWIA + TX PUC + CIRCIA CONTROL FRAMEWORK

The Compliance Layers at TX Multi-Utility Scope

Six regulatory tracks, each with its own separate compliance posture. The total compliance surface is broader than NERC CIP alone — and the parallel-narrative incident-response workflow is the structurally most-tested operational capability during audits. AWIA RRA / ERP authorship demands SCADA cybersecurity + treatment-process + customer-data — none of these map cleanly to NERC CIP scope.

01. NERC CIP-002–CIP-014

CIP-002 BES Cyber System identification, CIP-005 ESP, CIP-007 system security, CIP-008 IR plan (tri-clock), CIP-010 configuration, CIP-011 information protection, CIP-013 supply-chain (shared-MSP), CIP-014 physical security (designated substations)

02. AWIA §2013 RRA + ERP

42 USC §300i-2 Risk & Resilience Assessment on 5-yr cycle + Emergency Response Plan; community water systems serving >3,300 in TX; SCADA cybersecurity + treatment-process + customer-data enumeration

03. TX PUC §25.367 (96-hr)

16 TAC §25.367 — TX electric utilities (IOUs, certain co-ops, ERCOT QSEs) PUCT cyber-incident notification within 96 hours of discovery; concurrent with CIRCIA's 72-hr for NERC-registered

04. CIRCIA 72-hr

6 USC §681d — covered entities in energy, water (serving >3,300), pipelines, LNG face 72-hr CISA cyber-incident reporting once final rule is effective; runs concurrent with CIP-008 + §25.367

05. TSA SD-Pipeline-2021-01D

Top 100+ hazardous liquid + natural gas pipeline operators + LNG facility operators — annual cybersecurity assessment + cyber-incident reporting obligation; smaller TX gas LDCs exempt

06. TDPSA §541 + §521.053

Texas Data Privacy and Security Act — utility customer billing PII + usage data enumeration; §521.053 breach-notification trigger; concurrent with TX PUC §25.131/§25.134 consent regime

SECTION 5 | TOP 5 MULTI-UTILITY ATTACK VECTORS

The Five Patterns TX Multi-Utility Operators Face in 2026

01 AMI Headend Vendor-Default Credential Reuse

AMI headend servers (Itron, Landis+Gyr, Sensus, Aclara) hold the operator's full customer-metering telemetry + mass-customer PII. Vendor-default credentials on AMI admin are documented on TX utility OT networks. CISA AMI / OT threat advisories 2024–2025 confirm AMI vendor credential compromise is the most-attacked TX utility surface. Volt Typhoon's documented interest in customer-metadata + grid telemetry makes AMI headend a primary target.

02 SCADA Recloser / Pump Station OT Compromise

SCADA-controlled reclosers (electric distribution) and pump stations (water / gas / sewer) operate on the operator's OT VLAN. Vendor-IT compromise (the BR Utility Supply / shared MSP pattern) cascades across multiple TX operators simultaneously. Credential rotation on legacy OT modem firmware is the structural mitigation; CIP-005 Electronic Security Perimeter boundary documentation is the NERC CIP-side response.

03 Customer-Portal BEC ACH Wire Diversion

Customer-service mailbox compromise !' fraudulent ACH payment redirection for major commercial customer (>=$100K typical). Verified Anchor 5 baseline: TX Rio Grande Valley gas LDC phishing+wire diversion 2024. Phishing-resistant MFA on portal admin + callback verification on payment redirection + ACH positive-pay on outgoing refunds + autopay change call-back — the standard defenses for utilities smaller than the TSA SD-Pipeline threshold.

04 Shared-MSP / Vendor-IT Supply-Chain Cascade

A single MSP credential compromise cascades across multiple downstream utility customers simultaneously (the BR Utility Supply / Baton Rouge shared-MSP pattern). NERC CIP-013 supply-chain cyber-risk management plan is the federal regulatory response. Shared managed-service providers handling OT-IT integration work create single-point-of-failure risk across multiple TX utilities.

05 GIS / Esri Utility-Network Credential Exposure

GIS / Esri utility-network platforms hold the operator's complete service-territory asset inventory: every meter, transformer, pump station, main, valve, substation. Credential compromise on the GIS exposes the operator's complete infrastructure layout — for mapping purposes — to attackers who would target physical infrastructure during a follow-on cyber-physical event. TX PUC §25.182 mapping concerns intersect with GIS exposure.

SECTION 6 | 30/60/90-DAY TRI-CLOCK HARDENING

What to Do — and When

30 DAYS

- Enforce phishing-resistant MFA (FIDO2/WebAuthn) on every CIP-scope system — customer-portal admin, AMI headend, GIS, SCADA admin, QSE portal, email, VPN, admin consoles
- Inventory admin accounts; vendor-default credential scan on AMI + SCADA + GIS (Itron, Landis+Gyr, Sensus, Aclara, Cooper, S&C, SEL, ABB, Esri); CIP-007 R5 baseline
- AWIA §2013 RRA baseline scoping; RRA on the 5-yr cycle; population-served >3,300 trigger assessment; vendor ecosystem baseline
- CIP-008 IR plan drafting with TX PUC §25.367 + CIRCIA + ERCOT QSE narrative templates pre-loaded

60 DAYS

- OT-IT VLAN segmentation with CIP-005 Electronic Security Perimeter boundary documentation; AMI headend + SCADA recloser + GIS EDR coverage
- Customer-portal BEC callback workflow + ACH positive-pay + autopay-change call-back; phishing-resistant MFA on portal admins
- CIP-008 IR plan tested against the tri-clock parallel-narrative scenario (CIP-008 + §25.367 + CIRCIA + ERCOT); 90-day forensic image preservation routine
- NERC CIP-013 supply-chain cyber-risk management plan synthesis for shared-MSP / vendor-IT cascade exposure

90 DAYS

- AWIA §2013 Risk & Resilience Assessment + Emergency Response Plan authored and BOM'd against EPA RRAN scope; SCADA cybersecurity + treatment-process + customer-data enumeration
- NERC CIP-014 physical security audit support (substation designation assessment first); security plan + verification documented where applicable
- CIP-008 / TX PUC §25.367 / CIRCIA parallel-narrative tabletop exercise with PUCT docket contact + ERCOT QSE contact + CISA CIRCIA POC
- AWIA RRA + ERP EPA-audit-ready; quarterly AWIA review cycle calendared; DWSRF + BRIC grant-line compliance restored

SECTION 7 | CORERECON APPROACH

Sentinel / Fortress / Command for TX Multi-Utility Operators (25–500 endpoints)

SENTINEL — $89/endpoint/month

Best for: Small-TX multi-utility operators (1–50 endpoints, MUDs, SUDs, water systems serving <3,300)

- 24/7 SOC monitoring — TX-resident, OT-aware analysts
- Next-gen EDR with phishing-resistant MFA on CIP-scope admin plane
- CIP-007 R5 baseline + audit-log retention
- AMI headend + customer-portal credential rotation playbook
- Annual security awareness training with completion records

FORTRESS — $109–$129/endpoint/month

Best for: MUDs + small IOUs + multi-utility OES firms (51–500 endpoints, AWIA in scope)

- Everything in Sentinel, plus:

' OT-IT VLAN segmentation + CIP-005 ESP boundary documentation

' AMI headend + SCADA recloser + GIS behavioral EDR coverage

' Customer-portal BEC callback workflow + ACH positive-pay

' CIP-008 IR plan authorship + TX PUC §25.367 + CIRCIA narrative templates

' Quarterly vCISO report to PUCT docket contact + ERCOT QSE contact

---

COMMAND — $2,500+/mo flat retainer

Best for: NERC-registered entities + AWIA in-scope multi-utility primes; federal-grant-funded procurement

' Everything in Fortress, plus:

' Dedicated vCISO (contracted as NERC CIP coordinator)

' AWIA §2013 RRA + ERP authored + EPA-audit-ready (5-yr cycle)

' NERC CIP-014 physical security audit support (substation designation)

' CIP-013 supply-chain cyber-risk management plan (shared-MSP)

' TDPSA §541 enumeration + §521.053 notification workflow

' Annual tri-clock CIP-008 / §25.367 / CIRCIA tabletop exercise

---

30-MIN CIP-008 SLA • SDVOSB • OT-AWARE TX MULTI-UTILITY SOC

Industry median time from detection to containment is 1–4 hours (SANS 2024 IR Survey). Volt Typhoon kill-chain window: 45–90 min per CrowdStrike 2024 Global Threat Report. TX PUC §25.367 96-hour clock starts from incident discovery. CoreRecon's contractual 30-minute IR SLA measures against the actual attacker speed — not the MSSP industry average — leaving 95.5 hours for parallel-narrative authoring across CIP-008, TX PUC §25.367, CIRCIA, and ERCOT QSE storylines. SDVOSB-certified (CVE-verified via VA VetCert); USMC veteran-led; SOC staffed with TX-resident analysts familiar with MUDs / SUDs / gas LDCs / multi-utility OES firms and the AMI / SCADA / GIS / customer-portal attack surface. Federal-grant procurement eligible (DWSRF / BRIC / RUS / DOE OE-000 SDVOSB set-aside pathway).

Book Free Multi-Utility Posture Review !’

https://corerecon.polsia.app/assessment | (800) 955-2596

' SDVOSB Certified | ' 30-Min CIP-008 SLA | ' TX Multi-Utility-Aware SOC — Corpus Christi | ' USMC Veteran-led | ' AWIA RRA / ERP Authored

CoreRecon | SDVOSB | 30-Min CIP-008 SLA | https://corerecon.polsia.app | (800) 955-2596

Sources: CISA/NSA Joint Advisory AA24-038A (Volt Typhoon, Feb 2024); CISA/FBI/EPA/MS-ISAC joint PLC advisory (Nov 2024 + Jan 2025 follow-ups); Halliburton Q4 2024 SEC 10-K; Brazos Electric Ch.11 filings 2021–2022 (US Bankruptcy SDTX) + FERC/NERC/ERCOT enforcement reports; Moore County TX / City of Dumas public statements Nov/Dec 2024; FBI IC3 BEC reporting dataset 2024 Q4; NERC CIP-002 through CIP-014; 42 USC §300i-2 (AWIA §2013); 16 TAC §25.367 (TX PUC); 6 USC §681d (CIRCIA); TSA SD-Pipeline-2021-01D series; 49 CFR Part 192 / 195; Texas Data Privacy and Security Act §541, §521.053; AWWA G430 / J100 / DWFR; 16 TAC §3.70 (RRC); TX PUC §25.131 / §25.134; EPA Risk and Resilience Assessment (RRAN) guidance; CrowdStrike 2024 Global Threat Report; Mandiant M-Trends 2024 dwell-time analysis; SANS 2024 IR Survey.