TEXAS ELECTRIC COOPERATIVES

CYBER THREAT BRIEF

CoreRecon Intelligence Report | June 2026

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

NERC CIP-003-9 + PUCT TCMP + RUS Loan Compliance

BRAZOS ELECTRIC: $2.1B CHAPTER 11 BANKRUPTCY — WINTER STORM URI

DMEA Colorado billing system offline 1+ month from cyberattack | NERC CIP-003-9 enforced April 2026 | 62-source verified brief

OT/IT convergence: DNP3 · Modbus · AMI smart meters · ERCOT QSE cyber-financial boundary

KEY EVENTS & COMPLIANCE CLIFF

Brazos Electric	**$2.1B Ch.11**	G&T coop | 16 distribution co-ops | 1.5M Texans | Uri bills	2021
DMEA Colorado	**Billing offline**	Rural coop cyberattack | systems down 1+ month | ICS bricked	Nov 2025
Colonial Pipeline	**6-day shutdown**	VPN credential compromise !' OT shutdown | IT/OT bridge failure	May 2021
NERC CIP-003-9	**April 2026**	Vendor MFA + supply chain requirements now apply to Low Impact BES	2026

APPLICABLE REGULATIONS

NERC CIP-003-9 (eff. Apr 2026) • PUCT §25.367 TCMP • USDA RUS Loan Conditions • TDPSA (eff. Jul 1, 2024) • ERCOT Protocol §16.19

FREE POSTURE ASSESSMENT — NO OBLIGATION

https://corerecon.polsia.app/assessment?industry=Electric+Cooperatives | (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 THREAT LANDSCAPE

Texas electric cooperatives face a compounding threat environment where financial stress from Winter Storm Uri, expanding OT/IT attack surfaces, a tightening regulatory compliance calendar, and thin internal security resources converge into a single, exploitable vulnerability window. The DMEA Colorado precedent closes the "it won't happen here" argument — a rural co-op, billing system offline 1+ month, ICS devices bricked, no OT security expertise on staff.

BRAZOS ELECTRIC — THE DEFINING FINANCIAL EVENT

- !’ Brazos Electric Power Cooperative: $2.1B in ERCOT invoices during Winter Storm Uri (Feb 2021) — $9,000/MWh emergency cap (~500x normal rate)
- !’ Filed Chapter 11 March 1, 2021 in US Bankruptcy Court, Southern District of Texas — serving 1.5M Texans across 68 counties
- !’ HILCO Electric Cooperative: $121M in Uri obligations post-securitization; SB 3 securitization mechanism allowed cost-spreading over time
- !’ Lesson for cybersecurity: co-op boards exposed to existential systemic risk now actively harden against ALL failure modes — cyber included

PRIMARY THREAT EVENTS & ACTORS

CRITICAL	Delta-Montrose Electric Association — billing system offline 1+ month. ICS devices bricked. Russia-linked intrusion. 34,000 meters. Mid-size TX coop equivalent.
CRITICAL	VPN credential compromise !’ 6-day pipeline shutdown. OT shutdown was consequence of IT breach. No ICS exploit needed. Direct TX co-op parallel.
HIGH	Dragos 2025 YIR: state-linked group conducting near-constant spear-phishing targeting industrial networks. ERCOT QSE credentials are a target.
HIGH	ICS/OT-specific wiper malware documented by Dragos — active in Ukraine OT environments. Establishes capability context for US rural utility targeting.

SECTION 2 — NERC CIP COMPLIANCE STACK

Most TX distribution cooperatives with G&T relationships fall into the Low Impact category under CIP-002. CIP-003-9 enforcement began April 1, 2026 — fundamentally changing that calculus. NERC penalties can reach $1 million per violation per day.

ENFORCEMENT NOW

- Extends meaningful governance to Low Impact BES Cyber Systems — the first time most TX co-ops face real CIP obligations
- Vendor electronic remote access controls: MFA required for any vendor accessing Low Impact OT environments
- Supply chain risk management documentation required for vendor procurement and access
- Reliamag: "most significant compliance change for low-impact systems in the history of the CIP standards"

MED/HIGH IMPACT

- Documented supply chain risk management plans covering procurement, vendor access, and component integrity
- Growing concern as co-ops deploy smart grid equipment from international suppliers (Delta Electronics, Moxa, others)
- CISA ICS advisories 2025-2026: Delta Electronics DTM Soft, CNCSoft, COMMGR — active vulnerabilities in field-deployed OT equipment
- CIP-002 scoping is most common foundational weakness in NERC enforcement (ThreeShield assessment data)

FUTURE DEADLINE

- FERC Order No. 907 signed June 26, 2025 — mandates active INSM within Electronic Security Perimeters
- Compliance deadline: September 2, 2028 for High/Medium Impact with ERC in Control Centers
- September 2, 2030 for other Medium Impact systems
- Most TX co-ops currently lack the capability required by this standard

LOAN CONDITIONS

- RUS loan conditionality increasingly references cybersecurity program maturity including NERC CIP equivalency
- ReConnect/BEAD programs carry cybersecurity compliance conditions for broadband-deploying co-ops
- CoreRecon SDVOSB status aligns directly with RUS TAB review requirements — advantage pure IT MSSPs cannot claim
- Co-ops with outstanding RUS loans have ongoing compliance obligation to demonstrate security program maturity

SECTION 3 — OT/IT CONVERGENCE ATTACK SURFACE

Electric cooperative SCADA environments are built on protocols designed for reliability, not security. DNP3 and Modbus transmit data without encryption or authentication. AMI creates a two-way data channel from meters to MDMS. Field crew laptops bridge IT and OT networks. Credential-based attacks (valid credentials, not exploits) account for 65% of successful OT intrusions.

Risk: CRITICAL

- %¸ DNP3 Auth (DNP3 SA) — encrypted authentication variant has uneven adoption across the TX co-op fleet
- %¸ Modbus TCP: no native authentication or encryption — susceptible to interception, spoofing, and replay attacks
- %¸ A single co-op may operate legacy RTUs (DNP3), modern IEDs (IEC 61850), and PLCs (Modbus) — each requiring different monitoring
- %¸ Standard IT SIEMs cannot parse industrial protocols; active scanning can crash PLCs — passive OT monitoring required

Risk: HIGH

- %¸ AMI two-way channel: meters !' MDMS via DNP3 or vendor-specific protocols — head-end systems connected to corporate networks
- %¸ ScienceDirect 2026: AMI systems operate across M2M, cooperative, and cognitive radio protocols with SG-CPS vulnerable at multiple points
- %¸ 10,000 residential solar inverters collectively providing 50MW: grid-significant but no single device meets NERC CIP BES threshold
- %¸ Without adequate segmentation from SCADA networks, a meter-based intrusion can provide lateral movement into operational systems

Risk: HIGH

- %¸ CMMS (Maximo, SAP PM) with work orders and equipment config data accessible from field laptops that also connect to co-op WiFi
- %¸ Laptops connect to co-op WiFi, access corporate email, and may connect to OT networks for firmware updates or configuration
- %¸ A field crew laptop compromised via phishing becomes an IT/OT bridge — the Colonial Pipeline attack vector
- %¸ Distributed geographic footprint + limited IT staff = highest field crew exposure in the TX co-op sector

SECTION 4 — ERCOT MARKET PARTICIPATION RISK

Every TX distribution cooperative participates in ERCOT's nodal market through a Qualified Scheduling Entity (QSE). The QSE interface handles both operational dispatch and settlement data — creating simultaneous physical grid disruption and market fraud scenarios from a single compromise. ERCOT's market participant list is publicly available, allowing attackers to map the weakest QSE-co-op link in the chain.

QSE Interface — Cyber-Financial Boundary

- QSE required for all market participants: balanced schedule submission, ancillary services bids, settlement with ERCOT
- QSE must maintain: ICCP telemetry links to ERCOT, MMS connectivity, 24/7 control center, NERC reliability compliance
- Most distribution co-ops outsource QSE function to a third party — creating a third-party cyber risk layer
- Compromise scenario: QSE credential theft !' simultaneous operational dispatch manipulation + financial settlement fraud

ICCP Telemetry and Settlement Data

- ERCOT directly polls settlement meters via Settlement Metering Operating Guide specifications
- ICCP links carry both operational telemetry (SCADA data) and market settlement data — OT/financial overlap
- QSE-co-op ICCP link compromise: (1) dispatch instruction manipulation, (2) settlement data alteration, (3) fraudulent bids
- ERCOT Protocol §16.19 cybersecurity incident notification framework — requires timely communication on market-affecting incidents

Post-Uri Market Structure Changes

- SB 2 (87th TX Leg.) overhauled ERCOT governance; SB 3 created $2.5B Texas Electric Securitization Corp
- Securitization mechanism reduced financial systemic risk but increased IT system documentation requirements
- Increased scrutiny on market participant conduct creates more reporting requirements requiring reliable IT systems
- Co-ops need reliable, monitored IT/OT environments to meet ongoing ERCOT reporting and participation obligations

SECTION 5 — INCIDENT RESPONSE REALITY

Most TX distribution co-ops operate with an IT director model: 1-3 IT staff, business-hours coverage, on-call rotation designed for physical outages — not cybersecurity events. A co-op experiencing ransomware at 2am Saturday has no internal escalation path that reaches a cybersecurity professional within an hour. Dragos 2025 YIR: 75% of ransomware incidents resulted in partial OT shutdown, 25% in full OT shutdown.

MUTUAL AID LIMITATIONS

- !’ APPA/NRECA Mutual Aid Network: designed for physical restoration (crews, equipment) — NOT cybersecurity incident response
- !’ ESCC Cyber Mutual Assistance (CMA) program: depends on peer utility availability during active incident — not a guaranteed SLA
- !’ NRECA RCCP training / DeNexus risk quantification / OT-CERT: tools and guidance — not a managed 24/7 SOC service
- !’ Realistic Friday-night incident options: call MSSP with multi-day onboarding OR rely on IT director's personal network
- !’ None of these options meet a 30-minute response SLA — the gap CoreRecon fills

COMPETITOR LANDSCAPE

FREE for <$100M co-ops	Platform + Neighborhood Keeper — no managed service. OT Watch adds managed monitoring at enterprise pricing. Accenture acquisition June 2026 changes vendor stability. CoreRecon complements Dragos for co-ops needing SOC action, not just detection.
Enterprise pricing	Broad CPS visibility but meaningful engineering resources required to deploy. Minimum deal size above self-serve co-op range. Federal/ large enterprise focus.
IT-first MDR	Do not natively understand DNP3, Modbus, IEC 61850 SCADA protocols. Catch IT-side ransomware but miss OT-specific attack patterns. Entry point, not OT coverage.
Current state	1-3 IT staff, business hours only, no 24/7 OT monitoring. Inadequate for NERC CIP-003-9 compliance. CoreRecon co-managed Command tier augments without replacing.

8 CONTROLS EVERY TX ELECTRIC COOPERATIVE NEEDS IN 2026

01

Document all Low Impact BES Cyber Systems, implement vendor MFA for remote access, and create supply chain risk management policy. CIP-003-9 enforcement is live — this is not optional. Missing documentation creates $1M/day/ violation exposure.

02

Air-gap or firewall SCADA/ICS networks from corporate IT networks. The Colonial Pipeline lesson: ransomware didn't hit the OT — the OT was shut down to prevent spread. Maintain documented segmentation as NERC CIP ESA boundary.

03

MFA on all remote access paths including VPN, vendor remote support sessions, ERCOT QSE interface, and any cloud-hosted operational systems. NERC CIP-003-9 specifically mandates vendor remote access MFA for Low Impact BES Cyber Systems.

04

Behavioral EDR on IT endpoints, supplemented by passive OT protocol monitoring (DNP3, Modbus, IEC 61850). Standard IT EDR does not parse industrial protocol anomalies. Required for meaningful NERC CIP incident detection.

05

WORM-compliant backup of billing/CIS system, SCADA historian, and member data. Offsite/air-gapped copy. Tested recovery. DMEA billing was offline 1+ month — a tested recovery plan is the difference between days and months.

06

Verify AMI head-end systems are segmented from SCADA operational networks. Monitor for anomalous AMI communication patterns. Smart meters represent the largest new attack surface for co-ops post-ARRA AMI deployment.

07

Written IR plan covering NERC CIP-008 requirements, ERCOT Protocol §16.19 incident notification, and PUCT TCMP self-assessment. Table-top test annually. After-hours escalation path to a 24/7 cybersecurity professional.

08

Protect ERCOT QSE credentials and MIS access with MFA, dedicated systems, and access logging. Map QSE-co-op data flow and document it in NERC CIP topology. A QSE credential compromise creates simultaneous physical and financial risk.

30 / 60 / 90 DAY ROADMAP

Days 1–30 — Stop the Bleeding

- !’ Complete NERC CIP-003-9 compliance documentation: identify all Low Impact BES Cyber Systems
- !’ Enable MFA on all remote access paths: VPN, vendor sessions, ERCOT QSE interface
- !’ Audit ERCOT QSE credential storage — dedicated system, access log, rotation schedule
- !’ Verify AMI head-end segmentation from SCADA operational networks

Days 31–60 — Harden the Environment

- !’ Deploy OT-aware monitoring supplementing IT EDR on corporate network
- !’ Document IT/OT network boundary — create or verify ESA documentation for NERC CIP
- !’ Write NERC CIP-008 incident response plan; map ERCOT §16.19 notification requirements
- !’ Test backup recovery for billing/CIS system — target RTO and document result

Days 61–90 — Operational Resilience

- !’ Table-top incident response exercise targeting ransomware-on-Saturday-night scenario
- !’ Complete supply chain risk management documentation per CIP-013 framework
- !’ Review RUS loan compliance documentation to include cybersecurity program evidence
- !’ Brief board on cyber risk posture: NERC CIP status, DMEA precedent, 30-min SLA value

CORERECON PRICING FOR TX ELECTRIC COOPERATIVES

SENTINEL

$89/endpoint/mo

- 24/7 MDR (Managed Detection & Response)
- EDR + SIEM + threat hunting
- NERC CIP incident log delivery
- Breach notification workflow support
- Best for: small co-ops, 1–2 substations

20 endpoints = $1,780/mo

FORTRESS

$109/endpoint/mo

- Everything in Sentinel
- 30-min IR SLA (live TX SOC)
- OT protocol monitoring supplement
- NERC CIP-003-9 Compliance Pack
- Best for: mid-size distribution co-ops

30 endpoints = $3,270/mo

COMMAND

$129/endpoint/mo

- Everything in Fortress
- Co-managed vCISO model
- NERC CIP documentation support
- Annual tabletop exercise included
- Best for: G&T co-ops, co-ops with IT directors

50 endpoints = $6,450/mo

vs. Dragos OT Watch: enterprise pricing • vs. Arctic Wolf: $250+/endpoint/mo • vs. national MSSP generalists without NERC CIP or OT expertise

SDVOSB status aligns directly with RUS loan compliance conditions — advantage no IT MSSP or OT specialist can replicate at this price point.

FREE POSTURE ASSESSMENT — NO OBLIGATION

30-minute call. We map your OT/IT environment, NERC CIP-003-9 gaps, and ERCOT QSE risk.

https://corerecon.polsia.app/assessment?industry=Electric+Cooperatives • (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 SOC-grade security for Texas electric cooperatives at $89–$129/endpoint — with NERC CIP, ERCOT QSE, and OT protocol expertise no national MSSP can match.