Texas Oil & Gas:
OT/ICS Ransom Era.

2026 Cybersecurity Reality for Texas Oil & Gas Operators — Halliburton $35M, Colonial Pipeline, TSA SD-02F (May 3, 2025), SEC Item 1.05 4-Business-Day, RRC 16 TAC §3.71 & Volt Typhoon IT/OT

$35M — Halliburton TX RansomHub Aug 2024 — SEC 8-K Item 1.05 confirmed direct loss

935% — YoY ransomware surge vs. oil & gas — Zscaler ThreatLabz 2025

May 3 — TSA SD-02F effective — Cybersecurity Implementation Plan (CIP) authoring required

4 day — SEC Item 1.05 cyber-incident disclosure clock from materiality determination

SECTION 1 | EXECUTIVE SUMMARY

Five-Clock Compliance & SCADA Air-Gap Myth

Halliburton $35M. Colonial Pipeline. SCADA air-gap myth validated. Pre-authorize the SCADA isolation decision before the incident. Five parallel narrative clocks after every material incident.

!’ Halliburton TX (Aug 20, 2024, Houston HQ) — $35M direct loss from RansomHub; SEC 8-K Item 1.05 filed within 4-business-day clock; SEC 10-K Q4 2024 disclosure confirmed; OT/IT convergence risk validated

!’ Colonial Pipeline (May 2021, Houston-origin) — 5,500-mile refined-fuels pipeline shut down for 6 days from a single reused VPN credential with no enforced MFA; ~$4.4M DarkSide ransom paid; first-ever U.S. East Coast fuel supply shutdown

!’ Newpark Resources (Woodlands TX, Oct 2024) — NYSE-listed oilfield services ransomware; SEC disclosure confirms continued TX OFS-adjacent operator targeting

!’ ENGlobal Corp (Houston TX, Nov 2024 – Jan 2025) — third-party SCADA integrator to multiple TX midstream operators; 6-week business outage per SEC update; documented third-party-integrator cascade pattern

!’ Dragos VOLTZITE 2024–2025 + Hanna UT Pump Station Texas — confirmed OT-level PRC activity cluster + PLC ransomware proof-point at a Texas pump station (Dragos case study)

!’ TSA SD-Pipeline-2021-01D series + SD-02F (effective May 3, 2025) — top 100+ hazardous liquid + natural gas pipeline operators + LNG facility operators; expanded set per each directive revision; 12-hour security directive cyber-incident reporting window

!’ SEC Item 1.05 4-business-day cyber-incident disclosure clock (effective December 18, 2023) — applies to any SEC-registered TX oil & gas issuer; materiality determination framework required

!’ CIRCIA 72-hour CISA cyber-incident reporting clock — covered entities in energy + pipelines; final rule pending; concurrent narrative with TSA SD-02F + SEC Item 1.05

!’ RRC of Texas 16 TAC §3.71 — TX Railroad Commission pipeline damage-prevention + incident notification; HB 1208 (2023) + SB 3 / SB 1928 (2025) explicitly authorize cyber-induced-release reporting pathway

!’ TDPSA §541 — utility customer usage/billing PII enumeration; gas LDCs + retail gas marketers + co-op operators face enumeration risk; §521.053 breach notification trigger

!’ Volt Typhoon (PRC state-sponsored) has maintained pre-positioning in U.S. energy + water IT/OT networks since 2021 per CISA/NSA Joint Advisory AA24-038A (Feb 2024); Dragos VOLTZITE documents cellular RTU/SCADA gateway credential compromise as primary targeting vector

!’ 49 CFR Part 192/195/194 (PHMSA gas distribution + transmission + response plans) + 30 CFR §250 (offshore OCS) + 49 USC 60101 (pipeline safety statutory authority) all extend the parallel compliance surface for TX midstream operators

SECTION 2 | TX OIL & GAS THREAT LANDSCAPE 2024–2026

Six Verified TX Oil & Gas Anchors

01 Halliburton TX — $35M RansomHub — Aug 2024

Houston HQ oilfield services major. Aug 20, 2024 confirmed RansomHub ransomware attack — corporate IT taken offline. Q4 2024 SEC 10-K disclosed ~$35M direct recovery cost; SEC 8-K Item 1.05 cyber-incident disclosure filed within 4-business-day clock from materiality determination. OT/IT convergence risk validated — corporate IT billing + OT-side procurement dependencies collapse the OT-IT separation in practice. Halliburton sets the operational template for any TX SEC-registered oil & gas Item 1.05 disclosure.

02 Colonial Pipeline — VPN Credential — May 2021

Houston-headquartered 5,500-mile refined-fuels pipeline — largest in U.S. Single reused VPN credential with no enforced MFA allowed DarkSide access to corporate IT network. Full pipeline shut down for 6 days; ~$4.4M ransom paid in BTC; entire U.S. East Coast fuel supply disrupted. DHS Senate HSGAC testimony confirmed the structural OT-IT billing dependency pattern (operators feared they could not stage pipeline restoration without the IT-side billing system). The legend that informed every subsequent midstream OT-IT cybersecurity architecture.

03 Newpark Resources Woodlands TX — Oct 2024

NYSE-listed oilfield services company with HQ in The Woodlands, TX. October 2024 confirmed ransomware attack. SEC 10-Q filing Q4 2024 + company press statement. The Woodlands TX OFS supply-chain concentration exposes multiple TX upstream Permian/Eagle Ford operators as affected downstream nodes. Confirms that NYSE-listed TX OFS firms continue to be in active targeting post-Halliburton.

04 ENGlobal Corp Houston TX — 6-Week Outage — Nov 2024 – Jan 2025

Houston TX-based automation + engineering services firm with midstream + upstream clients. November 2024 ransomware attack — business operations remained offline for ~6 weeks per Jan 2025 SEC update. ENGlobal is a third-party SCADA integrator — its compromise cascades across multiple downstream operator clients. This is the documented third-party-SCADA-integrator cascade pattern; the same vendor-IT cascade model documented for IT-only MSP compromises, but for OT-integrator shops specifically.

05 Dragos VOLTZITE — Cellular RTU Gateway — 2024–2025

Per Dragos 2024 + 2025 ICS/OT threat intelligence, VOLTZITE is a PRC state-sponsored activity cluster specifically tracking cellular RTU/SCADA gateway credential compromise + Modbus/DNP3 read-and-write reconnaissance + persistence in IT networks adjacent to OT VLANs. Targets U.S. energy including oil & gas; pattern documented across multiple states including Texas. Many TX midstream operators do not have an inventory of their cellular RTU fleet — leading to OT assets operating outside CISO scope and outside any existing IR playbook after VOLTZITE pre-positioning.

06 Hanna UT Pump Station Texas — PLC Ransomware — 2024

Dragos-public case study of confirmed PLC ransomware affecting a Texas pump station. OT-level proof that pre-positioned compromise of TX oil & gas OT is real and not theoretical — the in-the-wild data point that justifies pre-authorizing SCADA isolation playbook adoption before any incident-disclosure clock starts. Specific named Texas pump station confirms the OT-VLAN compromise pattern; standard incident-response playbooks that treat OT as unreachable during incident response do not apply.

SECTION 3 | TSA SD-02F + SEC ITEM 1.05 + CIRCIA + RRC §3.71 + TDPSA + CMMC COMPLIANCE GAPS

Why Most TX Oil & Gas Operators Fail the Five-Clock

Five overlapping regulatory tracks independently enforceable — each capable of stopping pipeline operations, blocking SEC Item 1.05 disclosure on time, landing in FDIC/EPA/PHMSA/PUCT/RRC enforcement simultaneously, or triggering SEC cleant-liability qui tam exposure. TX oil & gas operators handling upstream E&P + midstream pipeline + gas processing + downstream refining contribute to all five tracks — and the most-tested operational capability during post-incident review is the parallel-narrative incident-response workflow.

TSA SD-02F CIP not authored

TSA Security Directive SD-02F (effective May 3, 2025) requires pipeline operators (expanded set per each directive revision) to author and maintain a Cybersecurity Implementation Plan (CIP) reviewable by TSA on a 12-hour window; to implement OT security controls (network segmentation + access control + ITA); to validate the CIP annually. CIP-as-drafted-not-template-fiction is the operational standard. CIP-gap exposure to TSA enforcement is unique among the five tracks because TSA enforcement can include operational directives with pipeline-shutdown authority.

SEC Item 1.05 4-business-day narrative authored post-incident

Halliburton precedent established the precedent: material cyber incidents disclosed within 4-business-day clock from materiality determination. Most TX oil & gas issuers lack a pre-defined materiality determination framework, a Form 8-K Item 1.05 drafting template, a parallel CIRCIA narrative, a parallel RRC §3.71 narrative, and the 90-day forensic image preservation routine. SEC enforcement on Item 1.05 specifically targets issuers who file late or under-disclose — the documented DOJ+SEC parallel-track exposure.

Pre-authorized SCADA isolation playbook missing

The Colonial lesson is pre-authorize the SCADA isolation decision before the incident. Most TX midstream operators lack a documented + tabletested OT-IT logical segmentation, hardware fail-safe modal hold on every RTU + PLC, instrumented state-machine restore + 4-hour OT-side manual fallback enabling pipeline operation without IT-side billing. Tested full isolation in under 30 minutes is the operational target — anything slower than 30 minutes puts the disclosure clock under operational pressure.

Cellular RTU/SCADA gateway inventory undocumented

Dragos VOLTZITE documents cellular RTU/SCADA gateway credential compromise as the primary PRC targeting vector for U.S. energy. Many TX midstream operators lack an inventory of their cellular RTU fleet at all — let alone vendor-default credential scans + firmware update validation + private cellular APN with strong per-device authentication. Cellular RTUs operate outside CISO scope today; VOLTZITE pre-positioning is invisible to current SOC visibility.

PI historian exfil defense not configured

OSIsoft PI / AVEVA PI historian servers collect every process measurement timestamp from across the

operator's OT fleet — flow rates, pressures, temperatures, valve states, tank levels. PI historian outbound traffic typically unmonitored — bulk-tag export alerts absent — and a compromised historian provides an attacker with complete operational visibility plus production-schedule planning capability. DLP-class enforcement + cryptographic integrity + 7-year retention is the structural response.

SECTION 4 | TSA SD-02F + SEC ITEM 1.05 + CIRCIA + RRC §3.71 + TDPSA CONTROL FRAMEWORK

The Compliance Layers at TX Oil & Gas Scope

Five regulatory tracks, each with its own separate compliance posture. The total compliance surface is broader than any single track — and the parallel-narrative incident-response workflow is the structurally most-tested operational capability during audit + post-incident review. SD-02F CIP authorship is not the same as SEC Item 1.05 disclosure; CIRCIA 72-hr CISA narrative is not the same as RRC §3.71 reporting; TDPSA §541 enumeration is not the same as CMMC 2.0 L2 SSP.

01. TSA SD-Pipeline-2021-01D + SD-02F (May 3, 2025)

Top 100+ hazardous liquid + natural gas pipeline operators + LNG facility operators. SD-02F requires CIP authoring + annual review + OT security controls + 12-hr CISA cyber-incident reporting window. Smaller TX gas LDCs exempt from TSA but bound by 49 CFR Part 192/195 PHMSA + RRC 16 TAC §3.71.

02. SEC Item 1.05 (4-business-day)

SEC Form 8-K Item 1.05 (effective December 18, 2023) — material cyber-incident disclosure within 4 business days of materiality determination. Applies to any SEC-registered TX oil & gas issuer. Halliburton Aug 2024 SEC 8-K precedent. Disclosure-no-later-than materiality determination applies.

03. CIRCIA 72-hr

6 USC §681d — covered entities in energy + pipelines + LNG face 72-hr CISA cyber-incident reporting once final rule is effective; runs concurrent with TSA SD-02F + SEC Item 1.05 + RRC §3.71 narratives. Parallel narrative authoring required.

04. RRC 16 TAC §3.71 (TX Railroad Commission)

TX-only regulator. HB 1208 (2023) + SB 3 / SB 1928 (2025 — Texas Oil & Gas Cybersecurity Initiative) explicitly authorize cyber-induced-release reporting to RRC. 16 TAC §3.71 is the operative rule. RRC-3000 portal submission template per core narrative workflow.

05. TDPSA §541 + §521.053 + CMMC 2.0

Texas Data Privacy and Security Act §541.002 enumerates sensitive PI categories — utility customer usage/billing PII; gas LDCs + retail gas markers + co-op operators face enumeration risk. §521.053 breach notification. CMMC 2.0 32 CFR Part 170 (where defense-adjacent — defense fuel supply chain) + DFARS 252.204-7012/-7021 72-hr double-clause + NIST SP 800-171 Rev 2 110 controls. SDVOSB co-prime advantage counts toward DFARS 252.219-7003.

SECTION 5 | TOP 5 TX OIL & GAS ATTACK VECTORS

The Five Patterns TX Oil & Gas Operators Face in 2026

01 VPN Credential Reuse (Colonial Trigger)

Single reused VPN credential with no enforced MFA on OT-adjacent IT systems is the documented Colonial May 2021 attack vector. Shared VPN accounts between IT and OT scopes, password rotation gaps, MFA bypass via SMS/call, contractor OT access via shared VPN without per-user provisioning — all occur in the typical TX midstream operator posture. Phishing-resistant FIDO2/WebAuthn MFA on every VPN credential is the structural mitigation.

02 Cellular RTU/SCADA Gateway Credential Compromise

Dragos VOLTZITE tracking documents credential compromise on cellular RTU/SCADA gateway as a primary PRC-sponsored targeting vector for U.S. energy. Fleet-wide RTU inventory + vendor-default credential scan + firmware validation + private cellular APN with strong per-device authentication + quarterly re-validation mitigates VOLTZITE pre-positioning across the TX midstream RTU fleet.

03 SCADA Vendor Remote-Access Credential Exposure

Emerson DeltaV / Honeywell Experion / Rockwell ControlLogix / Schneider Wonderware / AVEVA remote-access endpoints run on aging modem firmware with documented vulnerabilities. ENGlobal Corp Nov 2024 third-party-SCADA-integrator cascade pattern documented — operator must inventory every vendor remote-access endpoint, rotate per-vendor credentials quarterly, jump-host mediation, recorded session capture.

04 PI Historian Exfiltration (Operational Telemetry Confidentiality)

OSIsoft PI / AVEVA PI historian exfiltration is the documented operational-telemetry confidentiality threat. Bulk-tag export alerts absent in default configurations; outbound traffic unmonitored; hash-of-record absent; no cryptographic retention integrity. Alert on bulk-tag export, outbound whitelist enforcement, quarterly review of historian access log, 7-year retention with cryptographic integrity per FERC + PHMSA recordkeeping requirements where applicable — the structural defense.

05 Modbus/DNP3/OPC-UA/EtherNet-IP Engineering Workstation Compromise

Engineering workstations running Pro/ENGINEER, AutoCAD Plant 3D, or AVEVA E3D provide access to OT configuration + engineering data. Modbus (TCP/502), DNP3 (TCP/20000), OPC-UA (TCP/4840), EtherNet-IP (TCP/44818 + UDP/2222) protocols broadcast across the OT VLAN with limited authentication. Compromise of an engineering workstation allows attackers to read live process state + write configuration that affects physical operations. EDR + read-only protocol enforcement + configuration-baseline monitoring is the structural mitigation.

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

What to Do — and When

30 DAYS

- Enforce phishing-resistant FIDO2/WebAuthn MFA on every VPN + admin console — Colonial pattern mitigated
- Inventory admin accounts; vendor-default credential scan on cellular RTUs + SCADA gateways + DeltaV / Experion / ControlLogix modems (Dragos VOLTZITE mitigation)
- TSA SD-02F baseline scoping — pipeline + LNG operator scope; SEC Item 1.05 materiality framework pre-loaded; CMMC L2 baseline (where defense-adjacent)
- SD-02F CIP drafting with SEC Item 1.05 + CIRCIA + RRC §3.71 narrative templates pre-loaded

60 DAYS

- OT-IT VLAN segmentation with hardware fail-safe modal hold; cellular RTU/SCADA gateway behavioral EDR coverage; PI historian outbound-traffic DLP enforcement
- Tabletested pre-authorized SCADA isolation playbook — tested full isolation in under 30 minutes with documented 4-hour OT-side manual fallback
- SD-02F CIP + SEC Item 1.05 + CIRCIA + RRC §3.71 + TDPSA §541 parallel-narrative tabletop exercise; 90-day forensic image preservation routine documented
- Cyber insurance posture alignment — every insurer-acceptable control documented for renewal; SCADA-aware SOC deliverable in service

90 DAYS

- TSA SD-02F Cybersecurity Implementation Plan authored and BOM'd against TSA 12-hour review window; OT security controls validated; CIP-as-drafted-not-template-fiction
- SEC Form 8-K Item 1.05 materiality determination framework in production; 4-business-day narrative dossier pre-built; quarterly tabletop exercise
- RRC 16 TAC §3.71 RRC-3000 portal submission template pre-loaded; pipeline-incident classification matrix aligned to HB 1208 + SB 3 / SB 1928 language
- Cyber insurance full-capacity renewal prepared; sub-limit ride-back documented; known-good OLB exclusion language negotiated

SECTION 7 | CORERECON APPROACH

Sentinel / Fortress / Command for TX Oil & Gas Operators (25–500 endpoints)

SENTINEL — $89/endpoint/month

Best for: Small-TX midstream operators (1–50 endpoints, gathering + processing operators, gas LDCs)

- 24/7 SOC monitoring — TX-resident, SCADA-aware analysts
- Next-gen EDR with phishing-resistant MFA on IT admin plane (Colonial pattern mitigated)
- VPN credential-rotation playbook + admin-baseline
- TSA SD-02F scoping (in-scope pipeline + LNG operator scope)
- Annual security awareness training with completion records

FORTRESS — $109–$129/endpoint/month

Best for: TX midstream operators + gas processing + defense fuel supply chain operators (51–500 endpoints, SEC Item 1.05 + SD-02F in scope)

- Everything in Sentinel, plus:

- OT-IT VLAN segmentation + hardware fail-safe modal hold
- Cellular RTU/SCADA gateway behavioral EDR coverage (Dragos VOLTZITE mitigation)
- Pre-authorized SCADA isolation playbook (tabletested, <30-min full isolation)
- PI historian outbound-DLP + SCADA vendor remote-access inventory
- Quarterly OT-aware threat hunts (Dragos VOLTZITE-aware)
- Quarterly vCISO report to operations + IT leadership

COMMAND — $2,500+/mo flat retainer

Best for: TX SEC-registered midstream + defense-adjacent fuel supply chain operators; SD-02F + SEC Item 1.05 + RRC §3.71 fully staffed

- Everything in Fortress, plus:
- TSA SD-02F Cybersecurity Implementation Plan authorship + annual review
- SEC Form 8-K Item 1.05 4-business-day disclosure workflow (Halliburton precedent-aligned)
- RRC 16 TAC §3.71 incident reporting pathway + RRC-3000 portal template

' CMMC 2.0 L2 SSP — where defense fuel supply chain (DFARS 252.204-7012 72-hr clock built in)

' TDPSA §541 enumeration coverage + §521.053 notification workflow

' Annual five-clock tabletop exercise with TSA docket contact + RRC docket + CISA CIRCIA POC

30-MIN SCADA-AWARE SLA • SDVOSB • TX OIL & GAS-AWARE SOC

Industry median time from detection to containment is 1–4 hours (SANS 2024 IR Survey). Colonial Pipeline 6-day shutdown repurposes the OT-IT billing panic into the SCADA isolation playbook pre-authorization requirement. TSA SD-02F specifies a 12-hour cybersecurity-incident reporting window once CIP is in place. SEC Item 1.05 specifies 4 business days from materiality determination. CIRCIA specifies 72-hr CISA. RRC §3.71 has its own internal deadlines. CoreRecon's contractual 30-minute IR SLA measures against the actual attacker speed — not the MSSP industry average — leaving 11.5 hours for parallel-narrative authoring across SD-02F, SEC Item 1.05, CIRCIA, and RRC §3.71 storylines (and 72-hour Cyber Insurance renewal posture). SDVOSB-certified (CVE-verified via VA VetCert); USMC veteran-led; SOC staffed with TX-resident analysts familiar with midstream pipeline operations, gas LDCs, defense fuel supply chain, OT-VLAN segmentation patterns, cellular RTU gateway credential compromise (Dragos VOLTZITE 2024-2025), and the parallel-narrative incident-response workflow required after Halliburton-pattern material incidents.

Book Free SCADA / OT Posture Review !’

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

' SDVOSB Certified | ' 30-Min SCADA-Aware SLA | ' TX Oil & Gas-Aware SOC — Corpus Christi | ' USMC Veteran-led | ' SD-02F + SEC Item 1.05 + RRC §3.71 Coverage

Sources: Halliburton Q4 2024 SEC 10-K + SEC 8-K Item 1.05 (filed Aug 2024) + RansomHub kill-chain profile (CrowdStrike 2024 Global Threat Report); DHS Senate HSGAC Colonial Pipeline testimony (June 2021) + CEO public statements + Elliptic BTC blockchain analysis; Newpark Resources SEC 10-Q + press statement (Oct 2024); ENGlobal Corp SEC filings + 8-K Item 1.05 (Nov 2024 + Jan 2025 update); Dragos 2024 + 2025 ICS/OT Threat Intelligence (VOLTZITE cluster + Hanna UT Pump Station Texas PLC ransomware case study); TSA SD-Pipeline-2021-01D series + TSA SD-02F (effective May 3, 2025) Cybersecurity Implementation Plan; SEC Item 1.05 (effective December 18, 2023) Form 8-K cyber-incident disclosure; CIRCIA (6 USC §681d, final rule pending) 72-hr CISA; RRC of Texas 16 TAC §3.71 + HB 1208 (2023) + SB 3 / SB 1928 (2025) Texas Oil & Gas Cybersecurity Initiative; TDPSA §541.002 sensitive PI enumeration + §521.053 breach notification; CMMC 2.0 32 CFR Part 170 + DFARS 252.204-7012 72-hr + DFARS 252.204-7021 + NIST SP 800-171 Rev 2; 49 CFR Part 192/195/194 (PHMSA gas distribution + transmission + response plans); 30 CFR §250 (offshore OCS); CISA/NSA Joint Advisory AA24-038A (Volt Typhoon, Feb 2024); Zscaler ThreatLabz 2025 ransomware report; Mandiant M-Trends 2024 dwell-time analysis; SANS 2024 IR Survey.