Texas Defense Contractors: CMMC Phase 2.

2026 Cybersecurity Reality for Texas Defense Contractors — CMMC 2.0, Volt Typhoon, ITAR & FCA Qui Tam

$1.4T	Booz Allen DIB scale — annual DoD prime contracting flows reachable via Tier 2/3 compromise
110	NIST SP 800-171 Rev 2 controls required at CMMC L2 (32 CFR Part 170)
$1.2M-$70M	FCA qui tam DoD cyber settlement band documented 2023–2025 (31 USC §§3729–3733)
72 hr	DFARS 252.204-7012 DIBNet disclosure clock from incident discovery

SECTION 1 | EXECUTIVE SUMMARY

The CMMC Phase 2 Enforcement Window

Volt Typhoon pre-positioned. Booz Allen $1.4T DIB scale. FCA qui tam $1.2M-$70M. DFARS 72-hr clock. ITAR exposure on shop-floor CAD.

!’ Volt Typhoon (PRC state-sponsored) has maintained pre-positioned access inside the U.S. DIB since at least 2021 — CISA/NSA Joint Advisory AA24-038A (Feb 2024)

!’ Booz Allen Hamilton DIB scale analysis: $1.4T in annual DoD prime contracting flows sit one Tier 2/3 supplier compromise away from a supply-chain cascade

!’ CMMC 2.0 Phase 2 enforcement begins November 2026 under 32 CFR Part 170 — DFARS 252.204-7021 makes CMMC certification a condition of award

!’ NIST SP 800-171 Rev 2 = 110 controls across 14 control families; CMMC L2 self-attestation or C3PAO assessment required for every CUI-handling DoD contract

!’ DFARS 252.204-7012 72-hr DIBNet reporting clock at https://dibnet.dod.mil starts from discovery, not detection; 90-day forensic image preservation required

!’ DFARS 252.204-7019/7020/7021 four-clause joint enforcement — SPRS score in PIEE must be current within 3 years; POA&M items cannot exceed 180 days

!’ ITAR §120–130 export-controlled technical data is CUI in most DoD contract contexts — but ITAR compliance is not satisfied by CMMC alone (22 CFR §127 unauthorized export on cyber exfil)

!’ False Claims Act qui tam — documented DoD cyber settlements $1.2M to $70M; 15–30% relator share; 31 USC §§3729–3733 FCI misrepresentation predicates

SECTION 2 | TX DIB THREAT LANDSCAPE 2024–2026

Five Verified DIB Anchors

01 Volt Typhoon — U.S. DIB Pre-Positioning — CISA AA24-038A

PRC state-sponsored actor living off the land inside U.S. critical infrastructure AND the Defense Industrial Base since at least 2021. Prioritizes ITAR-controlled technical data and DoD program schedules. Texas ranks #2 in active defense suppliers per DoD OUSD(A&S) DIB supplier data — squarely in targeting set.

02 Booz Allen $1.4T DIB Scale — 2024 Sector Analysis

Documents $1.4T in annual DoD prime contracting flows reachable in a single Tier 2/3 supplier compromise. Supply-chain cascade concentrated in manufacturers and engineering services subs lacking prime-level SOC. TX hosts Lockheed, L3Harris, Raytheon, Boeing Satellite + sub-tier networks across DFW, San Antonio, Houston.

03 DoD Prime CMMC DRP Waiver Denials — 2024–2025

Multiple DoD primes formally denied CMMC Deficiency Remediation Plan (DRP) waiver requests from sub-tier contractors in 2024–2025. A 60–88 SPRS score at bid no longer qualifies for POA&M extension at prime discretion. Contracting officer has full authority to disqualify the bid before 72-hour DIBNet clock starts.

04 False Claims Act Qui Tam DoD Settlements — 2023–2025

DoD enforcement actions for cybersecurity representation false claims — smallest published settlement $1.2M, largest over $70M. Qui tam relators (often former employees) collect 15–30% of recovery. Falsely attesting to CMMC L2 compliance in SPRS while CUI remains unencrypted is the textbook FCA predicate under 31 USC §§3729–3733.

05 InterConnect TX F-16 Wiring Cascade — Ongoing

One of only 5 worldwide F-16 wiring licensees operates in TX DIB. Cyber incident at any F-16 wiring supplier producing conceptually identical assemblies would trigger functional kill flags across the global F-16 fleet. Prime-program-of-record + ITAR + CMMC + DFARS quadruple intersection — zero tolerance for CUI ledger variance.

SECTION 3 | CMMC + DFARS + ITAR + NIST 800-171 COMPLIANCE GAPS

Why Most TX Defense Contractors Fail the November 2026 Deadline

CMMC 2.0 Phase 2 enforcement under 32 CFR Part 170 (effective Dec 16, 2024) makes CMMC certification a condition of award on every CUI-handling DoD contract. Five overlapping regulatory tracks independently enforceable — each capable of pulling a contract, blocking an award, or landing the contractor in FCA qui tam litigation. The contracting officer in PIEE checks SPRS score before award; the DoD CIO checks the DIBNet disclosure narrative afterward.

CMMC L2 SSP not authored

32 CFR Part 170 + DFARS 252.204-7021 require a System Security Plan that reflects actual controls. Most primes and sub-tier suppliers have a template SSP, not a real one. The C3PAO assessor reads the SSP first — template fiction fails on day one.

SPRS score below prime-discretion floor

DFARS 252.204-7019/7020 require a current SPRS submission in PIEE before award. SPRS "d88 is the practical C3PAO-required floor across most DoD primes. Scores below +88 are the most common cause of bid disqualification documented in 2024–2025.

No 72-hr DIBNet disclosure workflow

DFARS 252.204-7012(c) requires rapid DoD reporting of cyber incidents affecting CUI. The 72-hr clock starts from incident discovery, not detection. Most contractors lack a pre-loaded DIBNet submission template with company CAGE code, contracting officer contact, and incident classification schema.

ITAR §120–130 tagging missing on CAD

CMMC covers CUI broadly but does not satisfy ITAR. Solidworks, AutoCAD, Siemens NX, CATIA shop-floor workstations frequently hold ITAR-controlled geometry. Foreign-national access block at OS level on tagged workstations must be enforced under 22 CFR §127.

No FedRAMP-equivalent cloud assessment

CMMC L2 requires FedRAMP Moderate equivalent for cloud services processing, storing, or transmitting CUI. Commercial M365 (any tenant not meeting FY 2024 procurement requirements) is NOT compliant for CUI storage at L2. Migration to GCC High / Azure Government / AWS GovCloud is the standard path.

SECTION 4 | NIST SP 800-171 REV 2 — 110 CONTROLS, 14 FAMILIES

The 14 Control Families at CMMC L2 Scope

NIST Special Publication 800-171 Rev 2 — "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations" — is the underlying control catalog CMMC Level 2 (32 CFR Part 170) aligns to. 110 controls across 14 control families. SPRS scoring is based on implementation status across every practice; score range -203 to +110.

01. Access Control

22 controls — boundary, remote, wireless, mobile code, separation of duties

02. Awareness & Training

3 controls — role-based training, insider threat awareness

03. Audit & Accountability

9 controls — auditable events, content of audit records, retention

04. Configuration Management

9 controls — baseline configuration, change control, least functionality

05. Identification & Authentication

11 controls — identifier management, MFA, biometric, replay-resistant auth

06. Incident Response

3 controls — IR plan, testing, training; DFARS 7012 72-hr clock integration

07. Maintenance

6 controls — controlled maintenance, nonlocal maintenance logging

08. Media Protection

9 controls — media access, marking, storage, transport, sanitization

09. Personnel Security

2 controls — screening, termination procedures

10. Physical Protection

6 controls — physical access authorizer, monitoring, visitor control

11. Risk Assessment

3 controls — system-level risk assessment, vulnerability scanning, remediation

12. Security Assessment

4 controls — control assessment plan, assessor independence, SSP maintenance, POA&M

13. System & Communications Protection

16 controls — boundary protection, cryptographic protection, session integrity, mobile code

14. System & Information Integrity

7 controls — flaw remediation, malicious code protection, monitoring, SP 800-161 CUI integration

SECTION 5 | TOP 5 DIB ATTACK VECTORS

The Five Patterns TX Defense Contractors Face in 2026

01 Volt Typhoon Living-off-the-Land

Per CISA/NSA AA24-038A, PRC state-sponsored Volt Typhoon uses built-in Windows admin tools, network admin utilities, and legitimate remote management platforms. Goal is CUI + ITAR technical data on a continuous basis, with latent capability to disrupt during geopolitical trigger. Signature-based EDR misses the activity — only behavioral SOC catches it.

02 CAD/CAM Shop-Floor Credential Theft

Solidworks, AutoCAD, Siemens NX, CATIA, Pro/ENGINEER workstations hold ITAR-controlled geometry, material specifications, and program-of-record assemblies. Credential theft from these workstations gives attackers direct CUI-bearing design IP. Volt Typhoon primary targeting pattern. Standard IT doesn't recognize CAD-credential reuse or DLL injection attempts in Solidworks macros.

03 Contractor Portal Account Takeover

GovWin, IUOO, DCMA audit portals, Wawf, PIEE — each login is a reconnaissance vector. Compromised GovWin identity lets attackers identify prime contract vehicle structures, option-year timing, and SPRS scores published to PIEE. Lateral movement from portal cred to DoD contract award intelligence is the modern DIB insider pattern.

04 Supply-Chain Vendor Compromise

Sub-tier engineering services and shop-floor manufacturers without prime-level SOC are the documented Booz Allen cascade root cause. A single Tier 2/3 supplier compromise exposes every prime contract assigned to that supplier. Volt Typhoon supply-chain pattern documented in AA24-038A — defense design IP is a primary target.

05 Remote Engineering VPN Bypass

Distributed engineering teams (TX firms often employ engineers across multiple states) access shop-floor CAD via VPN and remote desktop. VPN credential compromise (documented CISA pattern) bypasses perimeter defenses and provides direct CUI file access. Remote engineering is the primary Volt Typhoon living-off-the-land vector — they use legitimate admin tools inside the contractor's own VPN.

SECTION 6 | 30/60/90-DAY CMMC PHASE 2 HARDENING

What to Do — and When

30 DAYS

- Enforce phishing-resistant MFA (FIDO2/WebAuthn) on every CMMC-scope system — Solidworks, GovWin/IUOO, PIEE, email, VPN, admin consoles
- Inventory admin accounts; enforce PAM on distributed engineering accounts; document ITAR-flagged workstation access review
- CMMC L2 baseline scoping against NARA CUI Registry; FedRAMP-equivalent cloud tenant assessment; commercial M365 migration plan
- Quarterly SPRS submission to PIEE with self-assessment evidence; POA&M items tracked to closure

60 DAYS

- CUI VLAN segmentation and boundary protection; east-west monitoring for lateral movement within CMMC scope
- Next-gen behavioral EDR on every workstation running Solidworks, AutoCAD, NX, CATIA, Pro/E, Revit, and the project-management workstations touching GovWin/IUOO/PIEE
- DLP-based ITAR classification tagging on shop-floor design files; foreign-national access block at OS level on tagged workstations
- DFARS 252.204-7012 72-hr DIBNet disclosure workflow authorship with pre-loaded DIBNet submission template

90 DAYS

- System Security Plan (SSP) authored and BOM'd against CMMC assessment boundary; reflects actual controls, not template fiction
- POA&M closed to "d110 net SPRS; CMMC L2 self-attestation documented; C3PAO readiness dry-run (Command tier)
- DFARS 252.204-7021 attestation prep; DFARS 252.204-7020 subcontractor flow-down audit packet delivered
- Annual tabletop exercise with DFARS 72-hr clock runbook signing; FCA qui tam exposure review with breach counsel

SECTION 7 | CORERECON APPROACH

Sentinel / Fortress / Command for TX Defense Contractors (25–500 endpoints)

SENTINEL — $89/endpoint/month

Best for: Sub-tier suppliers (1–50 endpoints, Tier 2/3 CUI handlers)

- 24/7 SOC monitoring — TX-resident, DIB-aware analysts
- Next-gen EDR with phishing-resistant MFA on CMMC-scope systems
- CUI Registry scoping + audit-log retention
- Quarterly SPRS submission to PIEE
- Annual security awareness training with completion records

FORTRESS — $109–$129/endpoint/month

Best for: Mid-size primes and sub-tier (51–500 endpoints, multiple CUI contracts)

- Everything in Sentinel, plus:

' CUI VLAN segmentation + DLP-based ITAR classification tagging

' Behavioral EDR on Solidworks / AutoCAD / NX shop-floor workstations

' FedRAMP-equivalent cloud tenant assessment

' DFARS 252.204-7012 72-hr DIBNet disclosure workflow authorship

' Quarterly vCISO report to contracting officer program manager

---

COMMAND — $2,500+/mo flat retainer

Best for: Primes + complex primes (100+ engineers, C3PAO assessment bound)

' Everything in Fortress, plus:

' Dedicated vCISO (contracted as security officer)

' System Security Plan (SSP) — authored & maintained

' POA&M full lifecycle management — "d180-day closure target

' C3PAO-readiness dry-run + evidence package

' DFARS 252.204-7021 attestation prep + SPRS score management in PIEE

' Annual tabletop exercise + DFARS 72-hr clock runbook signing

---

30-MIN DFARS 7012 SLA • SDVOSB • DIB-AWARE TX 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. DFARS 252.204-7012 72-hour DIBNet clock starts from discovery. CoreRecon's contractual 30-minute IR SLA measures against the actual attacker speed — not the MSSP industry average — leaving 71.5 hours for forensic preservation, scope analysis, and DIBNet disclosure narrative accepted by the DoD CIO reviewer. SDVOSB-certified (CVE-verified via VA VetCert); USMC veteran-led; SOC staffed with TX-resident analysts familiar with DFW aerospace, JBSA-area primes, San Antonio cyber primes, and the Booz Allen DIB supply-chain pattern.

Book Free CMMC Posture Review !'

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

' SDVOSB Certified | ' 30-Min DFARS 7012 SLA | ' TX DIB-Aware SOC — Corpus Christi | ' USMC Veteran-led | ' CMMC L2 SSP Authored

Sources: CISA/NSA Joint Advisory AA24-038A (Volt Typhoon, Feb 2024); 32 CFR Part 170 (CMMC 2.0 Final Rule, effective Dec 16, 2024); DFARS 252.204-7012 (cyber incident reporting); DFARS 252.204-7019/7020/7021 (NIST SP 800-171 self-assessment + CMMC condition of award); NIST SP 800-171 Rev 2 (110 controls, 14 families); 22 CFR §§120–130 + §127 (ITAR export-controlled technical data); 31 USC §§3729–3733 (False Claims Act qui tam); Booz Allen Hamilton DIB sector economic analysis 2024; SPRS (Supplier Performance Risk System, PIEE); Lockheed Martin F-16 supplier licensing records; SANS 2024 IR Survey; CrowdStrike 2024 Global Threat Report.