nexustek

Cybersecurity Maturity Model Certification (CMMC) 2.0 Compliance Services

CMMC 2.0

COMPLIANCE FOR DoD MANUFACTURERS AND SUPPLY CHAIN

1%

of defense contractors feel fully prepared for CMMC audits[1]

89%

of contractors have already suffered financial, reputational, or business losses from a cyber incident.[1]

80K

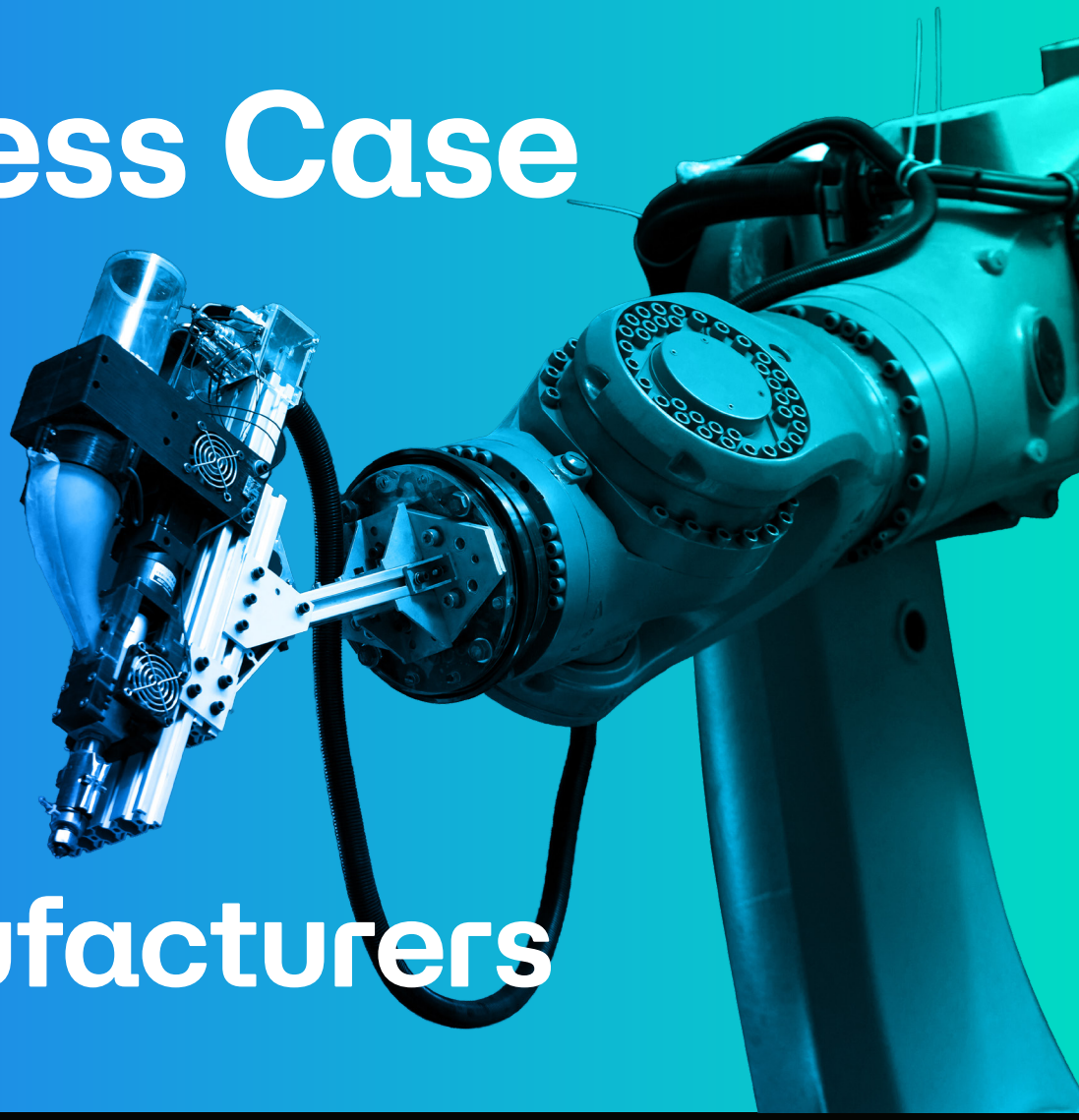
contractors need Level 2 certification. Only 270 hold a final CMMC certificate.[2]

1 Source: *Merrill Research / CyberSheath, State of the DIB Report*, 2025/2026

2 Source: *CyberSheath, 1% Ready for Deadline*, Sept 2025

The Business Case

CMMC 2.0 is a contract requirement. Manufacturers that handle Controlled Unclassified Information (CUI) or Federal Contract Information (FCI) on DoD contracts must achieve and maintain compliance or lose contract eligibility.



Where Manufacturers Are Exposed

CAD, PLM, and engineering environments

Technical data repositories — drawings, BOMs, process sheets, and revision-controlled files — are the primary home for CUI. Access control, audit trails, and secure boundaries are required.

Shop-floor and production endpoints

Operators access build instructions, test procedures, and inspection data at point of use. Every terminal with CUI access is in scope unless properly controlled or isolated via VDI.

Vendor and integrator remote access

CNC maintenance, robotics support, Manufacturing Execution Systems (MES) integration, and OEM access paths are common on the plant floor and frequently less controlled than corporate IT. CMMC scope follows the access path.

Shop-floor and production endpoints

Operators access build instructions, test procedures, and inspection data at point of use. Every terminal with CUI access is in scope unless properly controlled or isolated via VDI.

Cloud and file sharing for engineering workflows

If a cloud service stores, processes, or transmits CUI, it must be FedRAMP Moderate authorized or equivalent. This directly affects where drawings are shared and how engineering changes are managed.

The NexusTek CMMC Solution Stack

Each service maps to required CMMC 2.0 control domains.

Endpoint Detection and Response (EDR)	**System & Comms. Protection; Incident Response** Monitors and protects CUI endpoints including engineering workstations and production-floor PCs. Provides continuous detection evidence required for Level 2 audit.
Identity and Access Management (IAM)	**Access Control, Identification & Authentication** Enforces least-privilege and role-based access to CUI systems, CAD environments, and PLM platforms. Produces the access logs assessors review during C3PAO audit.
Multi Factor Authentication (MFA)	**Identification & Authentication** Mandatory for all accounts accessing CUI, including remote vendor and integrator access paths. No alternative implementation path exists at Level 2.
Managed Detection and Response (MDR)	**Incident Response; Audit & Accountability** 24/7 threat monitoring with documented incident response activity. Covers both IT and production-support environments.
AI Email Security	**System & Comms. Protection** Filters and monitors email-based file transfer, a primary channel for engineering drawings and technical packages moving to suppliers.
Private Cloud	**System & Comms. Protection; Config. Mgmt.** FedRAMP-equivalent controlled environment for CUI storage. Supports CMMC boundary definition, engineering document sovereignty, and data residency requirements.
vCISO	**Risk Assessment; All Domains** Owns SSP, POA&M, and scoping decisions including CUI enclave design for manufacturing environments. Sustains compliance between assessment cycles.

The NexusTek Engagement Model

01

READINESS ASSESSMENT

Gap analysis across all 110 controls. Supplier Performance Risk System (SPRS) score baseline. Remediation roadmap.

02

REMEDIATION + IMPLEMENTATION

Technical control deployment. System Security Plans (SSPs) and Plans of Action and Milestones (POA&Ms) documentation for NIST 800-171, and CMMC 2.0

03

AUDIT READINESS

C3PAO pre-assessment prep. Evidence package. Ongoing vCISO governance.

Why NexusTek

30+ years
IT SERVICES EXPERIENCE

1,200+ clients
98% SATISFACTION RATING

Tier 4 & 5 Private Cloud
99.9% uptime SLA. Controlled hosting environment supporting CMMC boundary definition and CUI data sovereignty.

Full-stack delivery
EDR, IAM, MFA, MDR, email security, Private Cloud, and vCISO under one partner. **No vendor coordination.**

AWARD-WINNING

THE CHANNEL CO. CRN TRIPLE CROWN WINNER

THE CHANNEL CO. CRN MSP 500 2026
10 YEARS IN A ROW

THE CHANNEL CO. CRN TECH ELITE 250 2025
8 YEARS IN A ROW

THE CHANNEL CO. CRN SOLUTION PROVIDER 500 2025
7 YEARS IN A ROW

Channel Partners. MSP501 2025 WINNER

Clutch — Top Managed Service Provider — Colorado 2024

Clutch — Top Dark Web Monitoring Company — United States 2024

Clutch — Top Cybersecurity Consulting Company — Colorado 2024

Clutch — Top Cloud Security Company — Colorado 2024

nexustek

Start with a CMMC Readiness Assessment

Establish your baseline. Identify gaps.
Get a prioritized remediation roadmap.

Learn more at nexustek.com

(877) 470-0401 • info@nexustek.com