SOLUTION BUILDERS

AN EBOOK FOR DEFENSE-SECTOR MANUFACTURERS

2026 EDITION

Updated for the 48 CFR Final Rule

The Manufacturer's CMMC Playbook.

What CMMC 2.0 means for your shop floor, why GCC High changes the conversation, and how to choose an IT partner that can actually get you certified before the 2026 deadline.

INSIDE THE GUIDE

01 / Why CMMC matters now

02 / The 2025-2028 compliance timeline

03 / The GCC High question, answered

04 / Choosing the right IT partner

PUBLISHED BY

Solution Builders · Bloomington, MN · sbinc.com

30+ YEARS · TOP 1% MSP · 98% CSAT

Your CMMC-ready technology partner

WHAT'S INSIDE

A four-chapter guide, written to be actionable.

Every chapter is built to be read on its own, but together they form the complete picture of what CMMC 2.0 requires of manufacturers, what the technology has to look like underneath, and what an IT partner needs to bring to the table.

01 **Why CMMC Now** — PAGE 04

The 2026 deadline, what CUI actually is, and why manufacturers are the most exposed tier of the DIB.

02 **The Compliance Timeline** — PAGE 09

Phase 1, Phase 2, and the road to November 2028, broken down so you know exactly when to start what.

03 **The GCC High Question** — PAGE 14

Why the cloud you choose can make or break your assessment, and when GCC High is no longer optional.

04 **Choosing the Right Partner** — PAGE 19

What SOC 2 and CMMC certification on your MSP actually buys you, and how Solution Builders helps you get certified.

SOLUTION BUILDERS

CHAPTER 01

01

Why CMMC, and why now.

The Department of Defense has spent six years moving from voluntary self-attestation to mandatory third-party certification. As of November 10, 2025, that transition is no longer theoretical. If your shop touches a defense contract, the clock is already running.

350K+
Suppliers in the Defense Industrial Base

110
NIST 800-171 controls required at Level 2

$300K
Top-end Level 2 remediation cost

9–12
Months typical to reach audit readiness

01 / WHAT IT IS

CMMC, in plain English.

The Cybersecurity Maturity Model Certification is the Department of Defense's way of verifying that contractors who touch government information are actually protecting it. Before CMMC, contractors self-attested. Now, they prove it.

The three things to know

01 **It replaces self-attestation.**

For nearly a decade, DoD contractors checked a box saying they followed NIST 800-171. Investigations found that many had not. CMMC introduces independent verification through Certified Third Party Assessor Organizations, or C3PAOs.

02 **It is tied to your contracts, not the calendar.**

CMMC becomes binding the moment it appears in a solicitation you want to bid on, or in an option year for a contract you already hold. For many primes, that is already the case.

03 **It flows down the supply chain.**

If you supply a tier-one prime like Lockheed, Boeing, or Northrop, your prime is now legally responsible for your compliance. They are auditing their subs. Heat treaters, plating shops, precision machinists, all of you, are in scope.

01 / THE LEVELS

Three levels. One that matters most to you.

CMMC 2.0 simplified the original five-tier model down to three. Most discrete manufacturers handling controlled information will land squarely at Level 2.

LEVEL 1

Foundational

17 controls

For contractors touching only Federal Contract Information (FCI). Annual self-assessment, basic cyber hygiene. The lightest path.

FCI ONLY · SELF-ASSESSMENT

LEVEL 2

Advanced

110 controls

Where most defense manufacturers land. Maps one-to-one to NIST SP 800-171 Rev 2. Third-party certification required for most CUI contracts starting November 2026.

CUI · C3PAO ASSESSMENT

LEVEL 3

Expert

110 + 24

For programs handling the most sensitive CUI under advanced persistent threat. Adds NIST SP 800-172 controls. Government-led assessment by DIBCAC.

HIGH-VALUE · GOVT ASSESSED

Most discrete manufacturers will need Level 2.

If a contract mentions DFARS 252.204-7012 or references CUI, plan for Level 2 and a C3PAO assessment.

01 / THE MANUFACTURING PROBLEM

Why the shop floor is the hardest part.

CMMC was written by people thinking about office computers. It is being enforced on shop floors. That gap is where most of the cost and risk lives.

Four manufacturer-specific risks

- **Legacy machines.**
  CNC machines running Windows 7 or proprietary firmware cannot enforce modern access controls, boundary protection, or integrity checking. If a program file with CUI loads onto that machine, the machine is in scope.
- **Mixed networks.**
  Most shops run one flat network. CMMC requires you to isolate CUI from general operations, which means real network segmentation, not just a VLAN slapped on top.
- **Paper-thin documentation.**
  Manufacturers operate on tribal knowledge. CMMC operates on written, dated, version-controlled artifacts. Assessors will not give credit for what is not documented.
- **Supply-chain flow-down.**
  If you outsource heat treating, plating, or finishing, those vendors must also meet your CMMC level. Your assessment now includes them.

73% **of the DIB**
is made up of small businesses. CMMC applies to all of them.

60% **of cyberattacks**
now target small and mid-size businesses, the very tier CMMC is designed to protect.

6–12 **months**
is the typical preparation timeline from kickoff to C3PAO readiness.

Sources: DoD CMMC Program Rule (32 CFR Part 170), Kiteworks 2026 DIB analysis, Cabrillo Club CMMC 2026 cost guide, VSO CMMC timeline research.

01 / THE COST OF WAITING

Doing nothing is the most expensive option.

Every quarter of delay compresses the timeline and inflates the cost of remediation. By the time CMMC appears in your contract, it is too late to start.

$50K–300K
Typical Level 2 program cost

20–40%
Cost premium when you rush remediation

0
DoD contracts awarded without certification by 2028

Three failure modes we see

- **Losing a recompete.**
  A prime renews your contract, the new option year adds DFARS 252.204-7021, you do not have a current SPRS score. The award goes to a sub that does.
- **Stop-work orders.**
  A prime audits its supply chain ahead of its own assessment. If you cannot produce a current SSP and POA&M, your work stops while you remediate.
- **Assessor backlog.**
  There are roughly 350,000 DIB suppliers chasing a small pool of C3PAOs. Assessment scheduling is already running 6 to 12 months out. Late starters wait at the back.

The bottom line.
If you handle CUI and you are not actively working toward CMMC certification today, you are running out of runway. The next chapter shows exactly how much time you have left.

CHAPTER 02

02

The compliance timeline.

The 48 CFR Final Rule took effect November 10, 2025. From that day forward, CMMC requirements began flowing into DoD solicitations, and a four-phase rollout has been ticking. Here is what each phase means for your business, and where you should be.

DEC 2024
32 CFR Part 170 Final Rule

NOV 2025
Phase 1 begins, Level 1 & 2 in contracts

NOV 2026
Phase 2 begins, C3PAO required

NOV 2028
Full implementation, no exceptions

02 / THE FOUR PHASES

Four phases. Three years. One window to act.

The DoD structured CMMC's rollout deliberately. Each phase expands the pool of contracts requiring certification and tightens what "certification" actually means.

PHASE 1 · Nov 10, 2025 — WE ARE HERE

Self-assessment era.

Level 1 and Level 2 (self-assessment) requirements begin appearing in DoD solicitations. Contractors must post current SPRS scores. DFARS clause 252.204-7021 is officially in play. If you handle FCI, your annual self-assessment is now a contractual obligation.

PHASE 2 · Nov 10, 2026 — 12 MONTHS TO GO

Third-party certification required.

C3PAO assessments become mandatory for most Level 2 contracts. Self-assessment is no longer an option for prioritized acquisitions. This is the deadline most manufacturers are racing toward.

PHASE 3 · Nov 10, 2027 — WIDER SCOPE

Level 3 enforcement begins.

DIBCAC-led Level 3 assessments are added for the most sensitive programs. Level 2 requirements expand into option years for existing contracts, not just new awards.

PHASE 4 · Nov 10, 2028 — FINAL DEADLINE

Full implementation.

Every applicable DoD contract requires the appropriate CMMC level as a condition of award or continuation. If you are not certified by this point, you are out of the defense supply chain.

02 / YOUR PERSONAL CLOCK

Where you should be, by quarter.

If you plan to bid on or hold contracts in 2027 and beyond, you need to be assessment-ready by Q3 2026. Work backward from that. The map below assumes a typical mid-size manufacturer with meaningful gaps.

Q2 2026

Scope and gap analysis.

Identify exactly where CUI lives. Inventory systems, build network diagrams, run a 110-control gap assessment against NIST 800-171.

Q3 2026

Design and budget.

Choose your cloud environment (Commercial, GCC, or GCC High). Build a remediation roadmap. Approve the budget. Engage your MSP.

Q4 2026

Build and migrate.

Stand up the secure enclave. Migrate users into it. Implement MFA, conditional access, logging, and encryption across the boundary.

Q1 2027

Document and train.

Finalize your System Security Plan. Build the evidence package. Train every user who touches CUI. Run incident response tabletops.

Q2 2027

Mock assessment.

Engage a Registered Practitioner or RPO to run a mock C3PAO assessment. Close any remaining POA&M items. Refine the SSP.

Q3 2027

C3PAO and certify.

Book your C3PAO assessment. Get certified. Begin the three-year cycle of annual affirmations and continuous monitoring.

Working backward, not forward.

Most manufacturers underestimate how long this takes. A realistic Level 2 program runs 12 to 24 months end-to-end. If you have not started a serious program by Q1 2027, you cannot be ready for a Phase 2 award in 2028.

02 / WHAT GETS LOGGED

SPRS scores, POA&Ms, and the paper trail.

CMMC is not just a checkpoint. It is a continuous reporting regime. Two artifacts will follow you for years: your SPRS score and your Plan of Action and Milestones.

SPRS

Supplier Performance Risk System

SPRS is the DoD's central database. Contracting officers check it before awarding or extending contracts. Your CMMC status and self-assessment score live here.

THE SCORING

110

Perfect score

One point lost for each unimplemented control. A score below 88 (POA&M minimum) may bar contract award.

POA&M

Plan of Action and Milestones

A POA&M lets you close certain gaps after assessment, but only for lower-weight controls and only within 180 days. Critical controls (1-point weighted, with rare exceptions) must be fully met up front.

THE WINDOW

180

Day closeout

All POA&M items must be closed and re-assessed within 180 days, or your conditional cert expires.

Three artifacts every assessor will ask for

- **System Security Plan (SSP).**
  A living document describing every system in your CUI boundary, how each of the 110 controls is implemented, and what its current status is. This is the single most important document in a CMMC assessment.
- **CUI data inventory.**
  Where CUI enters your network, where it lives, where it leaves. Network diagrams. Data flow diagrams. System inventories. Vague descriptions are an automatic finding.
- **Evidence package.**
  Logs, policies, configuration baselines, training records, incident response runbooks. "If it is not documented, it does not exist," is the assessor's golden rule.

02 / CHAPTER SUMMARY

Three things to take from this chapter.

01

Your deadline is not 2028. It is whenever the next contract you want appears.

Phase 2 (November 2026) is the most-cited milestone, but in practice your real deadline is set by your earliest target solicitation or option year.

02

12 to 24 months is the honest preparation window.

Anyone telling you it can be done in 90 days is selling you something. Real remediation, real documentation, and real assessment scheduling all take time.

03

The paper trail is permanent.

SPRS scores, SSPs, POA&Ms, and annual affirmations follow you for the life of your CMMC status. Building this system once, well, is far cheaper than rebuilding it later.

Sources for Chapter 2: 32 CFR Part 170 CMMC Program Rule (Dec 2024), 48 CFR Final Rule (Sept 2025), DFARS 252.204-7021 (effective Nov 10, 2025), Cyber AB CMMC Assessment Process, Workstreet 2026 deadline analysis, Secureframe CMMC timeline reference.

CHAPTER 03

03

The GCC High question.

Microsoft offers three different versions of Microsoft 365: Commercial, GCC, and GCC High. Most contractors discover the difference too late, after the wrong tenant has already been deployed. Picking the right one up front saves six figures and six months.

3
Microsoft 365 environments to choose from

325+
FedRAMP Moderate controls in the foundation

$100K+
Cost to rebuild a CUI environment from scratch

3–6
Months for new features to reach GCC High

03 / THE THREE ENVIRONMENTS

Commercial, GCC, GCC High, side by side.

These are not three flavors of the same product. They run on different infrastructure, are staffed by different people, and meet different compliance frameworks. Choosing wrong means either overpaying or building your compliance program on an insufficient foundation.

	COMMERCIAL	GCC	GCC HIGH
Infrastructure	Global Azure	Azure Commercial (US)	Azure Government (US-only)
Data residency	Global	United States	United States only
Operator citizenship	Global staff	May include non-US	Screened US citizens only
FedRAMP level	Moderate	Moderate	High
DFARS 252.204-7012	Insufficient	With config	**Yes (designed for it)**
CMMC Level 2 CUI	Not appropriate	Conditional	**Yes**
ITAR / EAR data	No	No	**Yes**
Available licenses	All tiers	Enterprise (E3/E5)	Enterprise only (no Business)
Relative cost	Baseline	~10-20% premium	~30-50% premium

If your contract touches CUI, GCC High is the safest path.

Commercial is not a viable foundation for Level 2. GCC works for basic CUI without export controls, but the moment ITAR or EAR enters the picture, GCC High becomes the only compliant option.

03 / WHEN YOU NEED IT

Five signals that point straight to GCC High.

GCC High is expensive. Picking it when you do not need it wastes money. Not picking it when you do can blow up your assessment. These are the unambiguous triggers.

01

Your contract mentions ITAR or EAR.

Export-controlled technical data, including CAD files, source code, and engineering drawings, must be restricted to US persons. GCC High is the only Microsoft 365 environment that guarantees this.

02

DFARS 252.204-7012(f) requires US-person support.

Sub-paragraph (f) governs incident forensics. If your contract demands US-only operator access, Commercial and standard GCC cannot satisfy it. GCC High can.

03

You handle CUI Specified (CUI//SP-XXX).

Certain CUI categories carry additional handling restrictions written into the source statute. These almost always require the sovereignty controls only GCC High provides.

04

Your prime explicitly requires it.

Many tier-one primes (Lockheed, Boeing, Northrop, RTX) now name GCC High in their supplier directives. If yours does, the conversation is over.

05

You expect to expand into CUI work.

Switching tenants is a six-figure migration. If there is any realistic chance you will handle CUI in the next 24 months, starting in GCC High avoids a painful tenant-to-tenant move later.

03 / THE FINE PRINT

What GCC High covers, and what it does not.

Buying a GCC High license does not make you CMMC certified. The platform handles part of the work. You and your IT partner handle the rest. Understanding the split is critical.

WHAT MICROSOFT COVERS

The platform layer.

GCC High provides FedRAMP High infrastructure, US-sovereign data centers, screened US-person operators, and the controls Microsoft attests to in its own SSP.

- FedRAMP High accreditation
- DoD IL4 / IL5 readiness
- US-only data residency
- Screened US-citizen operators
- Encryption at rest and in transit
- Underlying access-control primitives
- Audit-log infrastructure
- DFARS 7012 (c) through (g) flow-down

WHAT YOU AND YOUR PARTNER COVER

Everything above it.

How GCC High is configured, governed, monitored, and documented in your SSP. Microsoft hands you the building blocks. You still have to assemble them.

- Conditional access policies
- MFA enforcement on every account
- Endpoint management (Intune)
- User provisioning and offboarding
- Log review and SIEM integration
- Incident response procedures
- Security awareness training
- SSP authoring and maintenance

GCC High is a foundation, not a certification.

Microsoft handles roughly half of the technical controls in NIST 800-171. The rest is your responsibility, and the wrong configuration of GCC High will fail an assessment just as fast as the wrong cloud.

03 / THE MIGRATION

A six-step path to GCC High.

Moving from Commercial Microsoft 365 to GCC High is not an upgrade. It is a full tenant migration. Done well, it takes 90 to 150 days. Done poorly, it can break collaboration for months.

01 **Eligibility validation.**
Apply to Microsoft's US Government Cloud Eligibility Team with your CAGE code or signed regulatory attestation. Approval is required before you can purchase GCC High licenses through an authorized reseller.

02 **Architecture and scoping.**
Decide who lives in GCC High and who stays in Commercial. Most manufacturers do not put every user in GCC High. An "enclave" model isolates CUI users and shrinks the assessment boundary.

03 **Tenant build-out.**
Stand up the new GCC High tenant. Configure Azure AD, conditional access, MFA, Intune, Defender for Endpoint, Purview Compliance Manager. Pre-stage SharePoint, Teams, and OneDrive sites.

04 **Data and identity migration.**
Move mailboxes, files, and identities from Commercial to GCC High. Cross-tenant migration is non-trivial. Use Graph API, PowerShell, and a structured cutover plan with rollback paths.

05 **Endpoint enrollment.**
Re-enroll every device that touches CUI in the new GCC High Intune tenant. Apply Autopilot profiles, compliance policies, and disk encryption baselines. This is usually the most user-disruptive step.

06 **SSP, training, and cutover.**
Document the entire environment in your System Security Plan. Train every user on the new tools and the new rules. Decommission CUI access in the old tenant. Begin continuous monitoring.

Sources for Chapter 3: Microsoft Service Trust Portal, Secureframe GCC High 2026 guide, Ignyte Assurance Platform on Microsoft 365 environments, BEMO 2026 Office 365 CMMC analysis, Vestige & Cabrillo Club GCC High buyer's guides.

SOLUTION BUILDERS

CHAPTER 04

04

Choosing the right partner.

Most local MSPs cannot get a manufacturer to CMMC Level 2. The required certifications, tools, and documentation discipline simply are not in the playbook of a general-purpose IT shop. Here is what to look for, and how Solution Builders is built for exactly this work.

SOC 2
Independently audited security posture

50+
Engineers on the SB fractional team

24/7
SOC monitoring and response

30+
Years partnering with growing businesses

04 / CERTIFIED PARTNER

Your MSP's own compliance matters.

When you outsource IT to a partner, that partner becomes part of your CMMC assessment boundary. Their security posture is now your security posture. If they cannot prove their own controls, you cannot prove yours.

TABLE STAKES

SOC 2

Type II

An independent auditor verifies that your MSP actually does what their policies say they do, every day, for an entire year. Without this, you are taking marketing claims at face value.

PURPOSE-BUILT

CMMC

Capable Partner

Familiar with NIST 800-171, fluent in GCC High, comfortable producing SSPs and POA&Ms, and able to sit at the table during your C3PAO assessment as part of your support team.

What to ask a prospective partner

? **Do you carry SOC 2 Type II?**
Ask for the report. Read the auditor's name and the period covered.

? **How many CMMC Level 2 environments do you operate today?**
Look for real numbers, not vague "we have helped clients."

? **Can you show me a redacted SSP you authored?**
If they have never written one, they will not write yours well either.

? **Do you have engineers with CCP / CCA credentials?**
Certified CMMC Professionals and Assessors signal real depth.

? **Are you a Registered Practitioner Organization (RPO)?**
RPOs are listed by the Cyber AB and bring an auditable pedigree.

? **What is your GCC High deployment experience?**
Look for tenant migrations, not just license resales.

04 / THE SOLUTION BUILDERS WAY

How we run CMMC for manufacturers.

Solution Builders has spent three decades helping growing businesses move forward on technology. Our CMMC program is built on the same principle, design the technology around the workflow, not the other way around.

R

Readiness

Gap assessment against all 110 controls, CUI scoping, network discovery, and a prioritized roadmap. You leave this phase knowing exactly what you need to do.

I

Implementation

GCC High build-out, enclave architecture, identity and endpoint hardening, MFA and conditional access everywhere, SIEM integration. The technical foundation.

S

SSP & Evidence

We author your System Security Plan, build the evidence package, and maintain it as a living document. Assessors will see real artifacts, not boilerplate.

E

Examination

Mock C3PAO, POA&M remediation, and seat at the table during your real assessment. We stay with you through certification and into continuous monitoring.

What manufacturers see in the first 90 days

Day 1
Kickoff and CUI scoping begin

Day 30
Gap assessment complete and reviewed

Day 60
GCC High tenant designed and staged

Day 90
Migration starts, SSP in draft

04 / WHY SOLUTION BUILDERS

Three decades of helping manufacturers move forward.

We are not your IT vendor. We are your technology partner, the way our existing manufacturing clients describe us. The numbers below are what that looks like in practice.

30+
Years partnering with growing businesses since 1995

Top 1%
Ranked in the top 1% of all MSPs nationwide

98%
Average client CSAT across all support tickets

50+
Engineers on the fractional team you can leverage

Real outcomes from comparable engagements

MANUFACTURING · 85 USERS

100+ hours of monthly downtime eliminated.

Co-managed IT, Azure migration, layered XDR, 24/7 help desk. Ticket volume dropped 60% in 90 days.

PROFESSIONAL SERVICES · 42 USERS

Ransomware attack contained in 22 minutes, zero ransom paid.

Managed backups, XDR, MDR-backed SOC. Containment in minutes, full restoration overnight, fully operational by Monday.

ARCHITECTURAL FIRM · 60 USERS

38% reduction in infrastructure cost, zero on-prem footprint.

Microsoft 365 + Azure migration with MFA and ITDR. Real-time collaboration across offices, hardware capex near zero.

04 / YOUR NEXT MOVE

Three ways to start, today.

Wherever you are on the CMMC journey, from "we just heard about this last quarter" to "we are six months in and stalled," the first step is the same: a conversation about where you actually stand.

01

CMMC Readiness Snapshot

Free 30-minute call. We review your current contracts, identify your likely CMMC level, and tell you honestly whether you should be pursuing Level 1 or Level 2. No commitment.

30 MIN · FREE

02

Gap Assessment

Two-week structured engagement. We map your CUI, score you against all 110 NIST 800-171 controls, and deliver a prioritized remediation roadmap with realistic cost and timeline ranges.

2 WEEKS · FIXED FEE

03

Full Managed CMMC Program

End-to-end. We design and implement your GCC High environment, author your SSP, run your POA&M, operate your SOC, and walk into your C3PAO assessment with you. Month-to-month.

60-DAY NOTICE · 3X ROI TARGET

Ready to start the conversation?

We will tell you exactly where you stand, what it takes to get certified, and whether we are the right partner to help you get there.

sbinc.com · (952) 230-1161 · Bloomington, MN

SOLUTION BUILDERS

CMMC is the price of admission. Certification is the competitive edge.

The manufacturers who treat CMMC as a strategic capability, not a compliance tax, are the ones who will keep winning DoD work after 2028. Everyone else exits the supply chain.

THE THREE THINGS TO REMEMBER

01 **Nov 10, 2026 is the C3PAO deadline.**
Third-party certification becomes mandatory for most Level 2 CUI contracts.

02 **GCC High is the safest cloud foundation.**
Required outright for ITAR and EAR data. Strongly recommended for any CUI workload.

03 **Your IT partner is in your assessment.**
Pick one with SOC 2 Type II and proven CMMC delivery experience, not a generalist.

START THE CONVERSATION

sbinc.com

(952) 230-1161 · Bloomington, Minnesota
Serving manufacturers across the United States since 1995

© 2026 Solution Builders, Inc. All rights reserved. CMMC, GCC High, and related marks are property of their respective owners.