THE CMMC REQUIREMENTS CRISIS

Urgent And Critical Requirements Every DoD Contractor Must Have In Place NOW To Protect Contracts, CUI, Revenue, And Reputation

PROVIDED AS AN EDUCATIONAL SERVICE BY:
John Hill
TechSage Solutions

3463 Magic Drive Suite 255
San Antonio, Texas 78229
210-582-5814
www.techsagesolutions.com

THE DoD CONTRACTOR CMMC REQUIREMENTS CRISIS

CMMC is no longer just "coming someday." It is now part of the contracting reality for companies that want to keep, win, or support Department of Defense work.

The Department of Defense established the CMMC Program to verify that contractors have implemented required security measures to protect Federal Contract Information and Controlled Unclassified Information. The 32 CFR CMMC Program rule became effective December 16, 2024, and DoD later finalized DFARS contractual requirements to put CMMC into solicitations and contracts.

Your company may be small. You may be a subcontractor. You may only handle drawings, specifications, engineering notes, HR data tied to a program, or technical files from a prime.

But if your work involves FCI or CUI, CMMC can become the gate between you and your next contract.

AND HERE IS THE HARD TRUTH:

You do not pass CMMC because you bought cybersecurity tools.
You pass because you can prove your systems, people, policies, and evidence meet the required level.

WHEN CMMC SHOWS UP IN YOUR CONTRACT, WILL YOU BE READY…OR SCRAMBLING?

It's unfair, isn't it?

For years, many DoD contractors were told to "work on NIST 800-171" or "get ready for CMMC." But many were not given a clear path. Some were told their MSP had it covered. Some were told a firewall, antivirus, and MFA were enough.

They are not enough.

CMMC is about documented, assessable security. It includes scoping, asset inventories, policies, procedures, system security plans, evidence, assessment results, affirmations, and ongoing maintenance.

The final DFARS rule requires offerors and contractors to post certain CMMC self-assessment results to SPRS before award when required, maintain the required CMMC status during contract performance, complete annual affirmations of continuous compliance, and identify contractor information systems that will process, store, or transmit FCI or CUI.

That means the question is no longer:
"Do we have cybersecurity?"

The real question is:

Can we prove we meet the CMMC level required by the contract?

“WE’RE JUST A SUBCONTRACTOR,” YOU SAY?

That is exactly where many companies get surprised.

CMMC does not only affect large primes. It can flow down to subcontractors and suppliers when their work involves protected information or systems supporting the contract.

DFARS 252.204-7012 requires the clause to be included in subcontracts involving operationally critical support or covered defense information, and it requires subcontractors to support cyber incident reporting obligations.

DFARS 252.204-7021 also requires contractors to flow down the correct CMMC level to subcontracts and other contractual instruments when applicable.

So, if your prime asks for proof of compliance, the answer cannot be:

“Our IT guy said we’re fine.”

The answer must be:

“Here is our scope. Here is our assessment status. Here is our SSP. Here is our evidence. Here is our affirmation. Here is how we protect your data.”

EXACTLY WHAT DOES CMMC REQUIRE?

CMMC has three levels.

1

LEVEL 1 – FOUNDATIONAL
For companies that handle Federal Contract Information. Level 1 is based on the safeguarding requirements in FAR 52.204-21. It requires a **self-assessment**, submission into SPRS, and **annual affirmation**. No POA&Ms are allowed for Level 1.

2

LEVEL 2 – ADVANCED
For companies that handle Controlled Unclassified Information. Level 2 requirements are identical to NIST SP 800-171 Revision 2. Depending on the contract, Level 2 may require either a self-assessment or a C3PAO third-party assessment.

3

LEVEL 3 – EXPERT
For selected higher-risk programs. Level 3 uses selected requirements from **NIST SP 800-172 and is assessed by the government through DIBCAC.**

CMMC is not a single product. It is a security program that must be scoped, implemented, documented, assessed, affirmed, and maintained.

REQUIREMENT 1:
KNOW WHERE YOUR FCI AND CUI LIVE

You cannot protect what you cannot find.
Before a company can honestly claim readiness, it must know:

- **Where FCI is stored.**
- **Where CUI is stored.**
- **Who can access it.**
- **Which systems process it.**
- **Which cloud platforms store it.**
- **Which vendors touch it.**
- **Which endpoints can reach it.**
- **Which facilities house it.**
- **Which users can download, print, email, or transfer it.**

CMMC scoping requires organizations to define the assessment scope before assessment. For Level 1, systems that process, store, or transmit FCI are in scope. For Level 2, CUI assets, security protection assets, contractor risk-managed assets, specialized assets, and out-of-scope assets must be handled according to the CMMC scoping rules.

If your CUI boundary is fuzzy, your CMMC readiness is fuzzy.

REQUIREMENT 2:
IMPLEMENT THE SECURITY REQUIREMENTS

For Level 2, CMMC points directly to NIST SP 800-171 Revision 2. NIST says those requirements apply to nonfederal systems and organizations that process, store, or transmit CUI, or that provide protection for those systems.

That includes practical protections such as:

- Access control
- Multi-factor authentication
- Least privilege
- Audit logging
- Configuration management
- Vulnerability management
- Incident response
- Media protection
- Personnel security
- Security awareness training
- System and communications protection
- System integrity monitoring

Here is where many contractors get into trouble: They implement tools, but not the full requirement.

For example, having MFA is good. But CMMC also cares who uses it, where it is enforced, whether exceptions exist, how privileged accounts are handled, and whether evidence proves it works.

REQUIREMENT 3:
BUILD THE EVIDENCE BEFORE THE ASSESSOR ASKS FOR IT

CMMC is not passed by good intentions.
It is passed with evidence.

Your evidence should show that controls are not only written down, but actually operating. That may include:

- System Security Plan
- Network diagrams
- Asset inventories
- CUI data flow diagrams
- Policies and procedures
- Access control records
- MFA enforcement screenshots
- Training records
- Incident response plan and test results
- Vulnerability scan results
- Patch reports
- Risk assessments
- Backup test evidence
- Audit logs
- Vendor and cloud service documentation
- POA&M documentation where permitted

If your documentation is outdated, incomplete, or scattered across emails and folders, your assessment can become painful fast.

REQUIREMENT 4: UNDERSTAND POA&MS BEFORE YOU DEPEND ON THEM

Many contractors assume they can pass now and "fix the rest later."

Be careful.

CMMC limits when POA&Ms are allowed. Level 1 does not permit POA&Ms. For Level 2, a conditional status is only allowed under specific scoring and requirement conditions, and the POA&M must be closed within 180 days or the conditional status expires.

That means you should not treat a POA&M like a safety net.

You should treat it like a short runway.

If the missing item is not POA&M-eligible, or if the gap cannot be remediated quickly, it can block your assessment result, your contract eligibility, or your ability to satisfy a prime.

REQUIREMENT 5:
MAKE SURE YOUR CLOUD, MSP, AND VENDORS DO NOT BREAK YOUR COMPLIANCE

This is one of the most overlooked CMMC problems.

You may have strong internal controls, but your cloud provider, MSP, help desk, backup provider, SOC provider, file-sharing platform, or subcontractor may still create compliance risk.

DFARS 252.204-7012 requires contractors using an external cloud service provider to store, process, or transmit covered defense information to ensure the cloud service provider meets security requirements equivalent to the FedRAMP Moderate baseline and supports incident reporting, malicious software handling, media preservation, forensic access, and damage assessment requirements.

Your MSP also matters. If your MSP administers, protects, monitors, or connects to systems in your CMMC scope, you need to understand how that provider affects your **assessment boundary and evidence.**

Do not assume your vendor is “CMMC-ready.” Ask them to prove it.

EXACTLY HOW CAN CMMC NON-READINESS DAMAGE YOUR COMPANY

1

LOST CONTRACT ELIGIBILITY

If a solicitation requires a specific CMMC status, your company may need that status before award, option exercise, or extension. The DFARS rule states that CMMC level requirements apply to contractor information systems that process, store, or transmit FCI or CUI, and it requires contractors to maintain the required status during performance.

2

PRIME CONTRACTOR FRICTION

Primes do not want weak links in the supply chain. If you cannot answer compliance questions clearly, they may see you as risk.

3

AUDIT FINDINGS AND EXPENSIVE REMEDIATION

Waiting until the last minute usually costs more. Emergency documentation, tool replacement, segmentation, evidence collection, policy development, and vendor cleanup can be disruptive.

4

INCIDENT REPORTING PRESSURE

DFARS 252.204-7012 requires covered cyber incidents to be rapidly reported within 72 hours of discovery. It also requires review for evidence of compromise and preservation of affected system images and relevant monitoring data for at least 90 days.

5

REPUTATION DAMAGE

In the defense industrial base, trust is currency. Once a prime, contracting officer, or teaming partner sees you as a compliance risk, it can be hard to recover.

IS YOUR CURRENT IT PROVIDER TRULY READY FOR CMMC? TAKE THE QUIZ

If your current IT provider cannot answer "YES" to these questions, your company may not be adequately prepared.

□ Have they helped you identify every system that processes, stores, or transmits FCI or CUI?

□ Have they helped you define your CMMC assessment scope?

□ Have they created or updated your System Security Plan?

□ Have they built a current asset inventory that separates CUI assets, security protection assets, contractor risk-managed assets, specialized assets, and out-of-scope assets?

□ Have they mapped your controls to the required CMMC level?

□ Have they collected assessment-ready evidence for each requirement?

□ Have they reviewed whether your cloud providers meet the requirements for CUI handling?

□ Have they confirmed whether their own tools, remote access, monitoring systems, or technicians affect your CMMC scope?

□ Have they implemented MFA across users, administrators, remote access, and critical systems?

□ Have they enforced least privilege and removed unnecessary administrator rights?

□ Have they documented how privileged accounts are created, reviewed, monitored, and removed?

THE QUIZ CONTINUES

□ Have they implemented centralized logging and shown you what is being reviewed?

□ Have they provided vulnerability scanning, patch reporting, and remediation tracking?

□ Have they helped develop and test your incident response plan?

□ Have they confirmed you can support the 72-hour cyber incident reporting requirement if needed?

□ Have they helped you build a POA&M only where POA&Ms are actually allowed?

□ Have they created a repeatable process for annual affirmations?

□ Have they trained your users on phishing, CUI handling, removable media, and reporting suspicious activity?

□ Have they helped you prepare leadership for the responsibility of affirming compliance?

□ Have they provided executive-level dashboards that show readiness, open risks, and remediation progress?

□ Have they explained what evidence an assessor will expect to see?

If the answer is “no” or “I’m not sure” on several of these, you do not just have an IT issue. You have a contract-risk issue.

A PREEMPTIVE CMMC READINESS ASSESSMENT: THE ONLY WAY TO KNOW WHERE YOU REALLY STAND

A CMMC readiness assessment is a structured review of your people, processes, systems, documentation, and evidence against the level your contracts require.

It should answer four critical questions:

- **What CMMC level applies to us?**
- **What systems are in scope?**
- **What requirements are not fully met?**
- **What evidence do we need before assessment?**

This should not be a casual conversation. It should result in a clear findings report, prioritized action plan, and executive summary that leadership can understand.

Your goal is not just to “get compliant.” Your goal is to protect contract eligibility, reduce audit surprises, and create confidence with primes, contracting officers, and internal leadership.

WHEN THIS CMMC READINESS ASSESSMENT IS COMPLETE, YOU WILL KNOW:

- Whether your company is likely Level 1, Level 2, or potentially Level 3 based on the information you handle and the contracts you pursue.
- Where FCI and CUI live inside your environment.
- Which systems, users, vendors, cloud services, and facilities are in scope.
- Whether your SSP is complete, accurate, and assessment-ready.
- Which CMMC requirements are met, not met, or need more evidence.
- Which gaps are urgent because they may not be POA&M-eligible.
- Whether your MSP, cloud provider, or subcontractors create hidden compliance risk.
- What must be fixed first to protect contract eligibility.
- What leadership needs to know before submitting an affirmation.

Everything discovered during the readiness process should be handled confidentially and professionally. The goal is not blame. The goal is clarity.

PLEASE…DO NOT WAIT UNTIL THE RFP DROPS

I know you are busy.

You have operations to manage, contracts to deliver, staff to support, primes to satisfy, and leadership asking for answers.

But CMMC is not something to push off until the month before an assessment.

By then, the hard work may be too compressed. The evidence may not exist. The scope may be wrong. The vendors may not be ready. The policies may not match reality.

Get the facts now. Know your level. Know your scope. Know your gaps. Know your evidence. Know your vendors. Know your path forward.

CONTACT US TODAY TO SCHEDULE YOUR CONFIDENTIAL CMMC REQUIREMENTS READINESS ASSESSMENT!

Visit www.techsagesolutions.com

Reach out directly at 210-582-5814

Or email at info@techsagesolutions.com

Dedicated to serving you,
John Hill
TechSage Solutions

P.S. Most contractors do not fail because they ignored security completely. They struggle because they assumed someone else had it handled. CMMC rewards proof, not assumptions. Let's get the proof in place before your next contract depends on it.