The Phase 2 *Reckoning*

A CMMC 2.0 Battle Plan for the Engineering Defense Industrial Base

TIM TIPTON JR.

Arctiq

November 10, 2026

Phase 2 of the CMMC 2.0 rollout begins.

Level 2 third-party certification (C3PAO) becomes a condition of award for most contracts that touch **Controlled Unclassified Information**. For roughly **93% of the CUI-handling Defense Industrial Base**, the era of self-attestation closes.

Why this session exists

Tim Tipton Jr.

Air Force Veteran

Director, Cybersecurity Transformation | Arctiq

Why this session exists.

Most CMMC briefings spend the hour reciting the rule.

This one spends it on the part nobody covers: where **CUI actually lives** inside an AEC environment, where **engineering firms are failing C3PAO assessments today**, and what the next ninety days have to look like.

No vendor pitch. No theater.

A G E N D A

What we'll cover in 45 minutes

01 **Where we are**

The 48 CFR rule, DFARS 252.204-7021, and the phased rollout

02 **What CMMC actually requires**

Levels, scoping, FCI and CUI

03 **CUI hiding in plain sight**

The AEC environment, in specifics

04 **Where firms are failing**

The patterns C3PAOs are flagging today

05 **The ninety-day battle plan**

Assess. Document. Operate. Affirm.

SECTION

01

THE STATE OF PLAY

Where we are.

The rule is in force. The clock is ticking. The runway is short.

Four phases. Three years. We are already in Phase 1.

Nov 10, 2025

PHASE 1

Level 1 and Level 2 self-assessments in new solicitations. Contracting officers may insert Level 2 C3PAO requirements at discretion.

WE ARE HERE

Nov 10, 2026

PHASE 2

Level 2 C3PAO certification required at award for contracts handling CUI. The hard line.

18 MONTHS OUT

Nov 10, 2027

PHASE 3

Level 2 certification extends to option exercises. Level 3 requirements introduced at award.

Nov 10, 2028

PHASE 4

Full implementation across all covered contracts.

Three documents you have to know by name

THE PROGRAM

32 CFR Part 170

Defines the CMMC Program: levels, model, assessment policy, affirmation requirements, and waiver authorities. Finalized December 2024.

THE CONTRACT CLAUSE

48 CFR / DFARS 252.204-7021

Makes CMMC a binding condition of contract award and continued performance. Effective November 10, 2025. The enforcement mechanism.

THE PROOF

SPRS + Affirming Official

Every system handling FCI or CUI requires a CMMC UID in SPRS. Annual affirmation of continuous compliance by a named official. No SPRS, no award.

SECTION

02

PLAIN ENGLISH

What CMMC actually requires.

Three levels. Two assessment paths. One thing that decides which one applies to you.

THE THREE LEVELS

Your level is decided by the information you handle, not by what you want to do.

LEVEL 1

1

INFORMATION

FCI only

BASIS

FAR 52.240-93 basic safeguarding

(15 controls)

ASSESSMENT

Annual self-assessment

LEVEL 2

2

INFORMATION

CUI

BASIS

NIST SP 800-171 Rev 2

(110 controls)

ASSESSMENT

Triennial C3PAO (most firms) or self-assessment (≈5%)

This is where most of the room lives.

LEVEL 3

3

INFORMATION

CUI requiring enhanced protection

BASIS

NIST SP 800-171 + 800-172 subset

(110 + select 800-172)

ASSESSMENT

DIBCAC assessment

FCI vs. CUI

FCI

Federal Contract Information

Information **provided by or generated for the Government** under a contract that is **not intended for public release**.

Excludes simple transactional information (invoicing, payments) and content the Government has already made public.

Triggers Level 1.

CUI

Controlled Unclassified Information

Unclassified information **the Government creates or possesses** that requires safeguarding or dissemination control under federal law, regulation, or policy.

Categories include export-controlled, critical infrastructure, defense, and privacy data, among others.

Triggers Level 2 (or Level 3).

T H E N U M B E R S T H A T M A T T E R

By the time you finish your coffee tomorrow.

110

NIST 800-171 Rev 2 requirements at Level 2

320

Discrete assessment objectives to demonstrate

93%

Of CUI-handling DIB will need a C3PAO at Phase 2

3 yr

Validity of a Level 2 C3PAO certification

Sources: 32 CFR Part 170, DoD program estimates, NIST SP 800-171A

SECTION

03

THE DIFFERENTIATOR

CUI hiding in plain sight.

If you can't point to your CUI, you can't scope it. If you can't scope it, you can't pass.

Where CUI shows up in AEC, before anyone calls it CUI

01	**Site & facility drawings**	DoD installation site plans, base utility maps, perimeter security designs, and access control layouts.
02	**BIM models**	Federated models containing geometry, MEP, and equipment data for controlled DoD facilities, ammunition storage, or SCIFs.
03	**ATFP design packages**	Anti-Terrorism Force Protection standoff calculations, blast analysis, and physical security countermeasure designs.
04	**Geospatial datasets**	Precise coordinates, aerial imagery, and survey data for DoD installations marked under DoDI 5200.48.
05	**Contract & specification packages**	Statements of work, technical exhibits, and submittal registers carrying CUI markings, distribution statements, or NOFORN.

The places nobody thinks to look

01	**Submittal transmittals**	Shop drawings, product data, and samples flowing between sub, prime, and DoD via consumer email tools you do not control.
02	**Daily reports & QC logs**	Field reports referencing facility purpose, security system installations, or controlled equipment by nomenclature.
03	**As-built drawings**	Final installation records for security systems, mass notification, and access control, often archived for decades.
04	**Construction photos**	Site photographs of DoD facilities under construction, captured on personal phones, synced to personal cloud accounts.
05	**Test & commissioning records**	Acceptance test reports, IPS/IDS performance data, and balanced magnetic switch tamper test results.

How to know whether you are looking at CUI

01

Is it marked?

Look for the banner: CUI, FOUO (legacy), or category markings (CUI//SP-CTI, CUI//SP-EXPT). Distribution Statements B through F on drawings are a strong signal.

02

Where did it come from?

Information generated for the Government under a DoD contract is presumed protected. If the prime sent it down, or if you produced it under a DoD SOW, treat it as CUI until proven otherwise.

03

What does the contract say?

DFARS 252.204-7012 obligations, CUI categories listed in Section J, and the contract's distribution statements tell you what you have and how to handle it.

SECTION

04

THE HARD PART

Where firms are failing.

C3PAOs are not failing firms on the exotic. They are failing them on the basics.

The five findings that sink engineering firms

01 **Thin SSP**

System Security Plans that read like a marketing brochure. Required granularity is per-objective, per-system, per-control. Most firms have neither the detail nor the diagrams to support it.

02 **Weak MFA coverage**

Phishing-resistant MFA on privileged accounts is non-negotiable. SMS codes do not clear the bar. Many environments still allow exceptions for service accounts and contractors.

03 **Encryption gaps**

FIPS 140-2 / 140-3 validated cryptography is required for CUI in transit and at rest. The product being marketed as 'FIPS-compliant' is not the same as having an active FIPS-validated module in operation.

04 **Logging without monitoring**

Generating logs is not the same as reviewing them. SIEM coverage, retention, and a documented review cadence are all explicit objectives.

05 **Boundary confusion**

If you cannot draw a diagram of where CUI enters, lives, and leaves your environment, your scope is undefined. Undefined scope means everything is in scope.

Your MSP is in your assessment whether they know it or not

If an outside provider stores, processes, or transmits your CUI, **they are inside your boundary**. Their controls become your controls.

CSPs (Cloud)

Cloud Service Providers handling CUI must be FedRAMP Moderate baseline or equivalent. A standard commercial Microsoft 365 or Google Workspace tenant does not clear that bar.

ESPs (Managed IT)

External Service Providers, including MSPs and MSSPs, are in scope when they manage assets that touch CUI. They need their own SSP coverage or you inherit the deficiency.

Shared responsibility

Customer Responsibility Matrices are non-negotiable. Every shared control needs a documented split of who does what, in writing, signed.

Your eligibility depends on suppliers DoD will not tell you about

The rule.

Primes must flow down CMMC requirements to **every subcontractor and supplier** whose performance involves FCI or CUI, at the **correct level for that sub's role**.

Subs must post their own assessments and affirmations to SPRS, but DoD does not share sub data back to primes. Primes must verify compliance independently.

The trap.

You are responsible for a chain you cannot see.

The specialty subs that engineering primes rely on most — door hardware, security electronics, acoustical, geotechnical — are precisely the firms least prepared and most likely to walk away from DoD work rather than certify.

Your bid pool is shrinking on a clock you do not control.

SECTION

05

THE PLAN

Ninety days, three movements.

Assess. Document. Operate. The same sequence that wins every military operation.

Assess. Find the ground truth before you write a word.

01	**Identify CUI and its custodians**	Walk every business unit. Map where CUI enters, lives, is processed, and exits. Name the systems and the people.
02	**Draw the boundary**	Define your CMMC Assessment Scope. Be aggressive about what you keep out: an enclave is cheaper than a perimeter.
03	**Inventory assets and people**	Categorize per 32 CFR 170.19: CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, Out-of-Scope.
04	**Inventory your ESPs and CSPs**	Every provider that touches your scope. Pull their CRMs and FedRAMP packages now, not at audit.
05	**Self-score against 800-171A**	All 320 objectives. Honest scoring beats heroic scoring every time.

Document. Build artifacts an assessor can read in a day.

01	**Draft the System Security Plan**	One SSP per assessed environment. Each of the 110 controls, each of the 320 objectives, with system names, configurations, and diagrams.
02	**Build the network and data flow diagrams**	Boundary, components, trust zones, CUI flow paths, ESP integrations. Assessors read these first. So should you.
03	**Sign the Customer Responsibility Matrices**	Every shared control with every ESP and CSP, formally executed. The shared responsibility myth dies here.
04	**Stand up the POA&M discipline**	Identify deficiencies you will remediate before assessment and those you will carry as POA&M (only certain controls eligible per 32 CFR 170.21).
05	**Lock the policies and procedures**	Eleven policy families minimum. Approved by the affirming official, version-controlled, accessible to staff.

Operate and affirm. Prove the program is alive.

01	**Run the program in the open**	Generate the evidence assessors want: log reviews, vulnerability scans, training records, access reviews, incident drills.
02	**Conduct a tabletop incident exercise**	The DFARS 7012 72-hour incident reporting obligation is not theoretical. Drill it. Document the after-action.
03	**Run a mock C3PAO assessment**	Best money you will spend before the real one. Either internal team or a CCP-led readiness assessment.
04	**Post and affirm in SPRS**	Submit your CMMC UID(s). Self-score where applicable. Have the affirming official complete the annual affirmation of continuous compliance.
05	**Schedule the C3PAO**	Authorized C3PAO bench is finite and filling. Book your assessment window now to land it inside Phase 2.

Four artifacts. No artifact, no eligibility.

SSP

System Security Plan

The book. 110 controls, 320 objectives, system context, diagrams, scope boundary. The single document your C3PAO will live inside for the duration of the assessment.

POA&M

Plan of Action & Milestones

The list of what is not yet done, who owns it, what it costs, when it closes. Required to move from Conditional to Final status.

SPRS

Supplier Performance Risk System

Your CMMC UID(s), your score, your affirmation, all current and posted. Contracting officers cannot award without it. Period.

AFFIRM

Annual Affirmation

The named affirming official certifies continuous compliance every twelve months. A perjury-bearing signature, not a checkbox.

T H E C O S T O F I N A C T I O N

What happens if you wait.

01 **Contract ineligibility**

Contracting officers are barred from award, extension, or option exercise without a current CMMC status posted in SPRS at the required level.

02 **Lost subcontract pipeline**

Primes drop subs that cannot demonstrate compliance. Lockheed, Northrop, and General Dynamics are already culling supply chains.

03 **Forfeit of competitive bids**

Engineering firms without certification cannot bid on most new DoD design and construction work after November 2026. The bid pool shrinks, and so does the win rate.

04 **Cost compounding**

Late-stage remediation under deadline pressure runs three to five times the cost of a deliberate ninety-day program.

C L O S I N G

The bid pool or the bench.

CMMC is not a cybersecurity initiative. *It is a market access program enforced by a contracting clause.*

On November 10, 2026, the engineering firms that did the work will keep bidding. The ones that waited will be on the bench, watching primes hand the project to someone else.

Do the work.

Q U E S T I O N S

Let's open it up.

Tim Tipton Jr., CISSP

Director, Cybersecurity Transformation | Arctiq

Las Vegas, NV

F O L L O W U P

CMMC readiness assessment
C3PAO preparation
vCISO engagement
Managed detection and response

Thank you, SAME Omaha.