

• STRATEGIC BRIEF · 2026

CMMC 2.0 isn't slowing down.

Neither can your readiness.

CMMC 2.0 will land in solicitations faster than the phased-rollout language suggests. For contractors handling CUI, the impact is immediate — without NIST 800-171 alignment and defensible documentation, contract pursuits stall or disappear.

110

NIST 800-171 CONTROLS

6–12 mo

window to get ready

Level 2

certification target

KEY TAKEAWAYS

Three things every defense contractor should know now.



CMMC REQUIREMENTS

Will appear in solicitations quickly after rule publication — much sooner than the "phased rollout" language suggests.



DOCUMENTATION MATURITY

Not security tooling, is the primary barrier preventing companies from passing Level 2 assessments.



EARLY PREPARATION

Reduces audit risk, lowers cost, and prevents disruptions to ongoing DoD contract pursuits.

THE FIVE INSIGHTS

What every contractor must understand now.

01

INSIGHT

Phased Rollout Will Move Faster Than Expected

Although the rule references a phased rollout, CMMC requirements will appear quickly in solicitations. Once contract clauses are available, agencies adopt them without delay. Level 2 requirements will surface on sensitive programs in weeks, not months. Organizations expecting a long transition period risk being unprepared.

02

INSIGHT

CUI Scoping Will Define Compliance Success

Accurately defining systems, assets, personnel, and processes that touch CUI is the most critical early step. Over-scoping drives cost and audit complexity; under-scoping creates compliance risk. Scoping discipline determines whether Level 2 is manageable or overwhelming — far more than individual control implementation.

03

INSIGHT

Documentation Maturity Drives Level 2 Outcomes

SSPs, POA&Ms, policies, procedures, diagrams, and evidence must be accurate and consistent. Most assessment delays stem from documentation gaps, not missing tools. Organizations that delay documentation face compressed timelines, audit stress, and costly remediation.

04

INSIGHT

C3PAO Availability Will Constrain Assessments

The number of authorized C3PAOs is increasing, but capacity remains limited. As more contractors pursue Level 2, competition for assessment scheduling will intensify. Early conversations provide scheduling flexibility and clearer expectations long before formal readiness.

05

INSIGHT

POA&Ms Are Not a Compliance Safety Net

POA&Ms allow limited flexibility for specific non-critical controls, but they cannot compensate for major gaps. Several high-weight controls are ineligible, and overreliance risks conditional certification failure. Treating POA&Ms as a fallback rather than an exception jeopardizes contract eligibility.

WHAT CMMC MEANS FOR LEADERSHIP

Strategic implications, by function.

CMMC is more than a cybersecurity requirement — it is an organizational readiness mandate that touches every major functional area. Leaders across the business will feel the impact differently.



STRATEGIC BUSINESS LEADERS

CMMC directly influences contract eligibility and revenue continuity. Treat compliance as an operational investment, not a technical project. Resourcing, staffing, and prioritization decisions must be made early — CMMC readiness is a defining advantage when bidding new work or recompetes.



TECHNOLOGY & SECURITY LEADS

Tech teams must plan for focused control remediation, documentation, and evidence collection. Many organizations will need to formalize processes that were historically informal. Clear ownership of control families across sysadmins, network engineers, and security is critical.



FINANCE & OPERATIONS

Budgeting for CMMC means understanding the cost of security enhancements, documentation development, external assessment fees, and staffing. CFOs should plan multi-phase budgets that support remediation now and sustain ongoing compliance after certification.



PROGRAM & CONTRACT MANAGEMENT

Contract teams will increasingly encounter solicitations with explicit CMMC levels. They must interpret requirements, assess readiness, and coordinate bid/no-bid decisions — while tracking subcontractor compliance, supply-chain risk, and flow-down responsibilities.

THE NEXT 90 DAYS





A practical plan, time-bound.

A sequence for organizations aiming to achieve or maintain Level 2 readiness.

30

 days





IN THE NEXT 30 DAYS

- 
Finalize CUI Scoping
 Align leadership on system boundaries.
- 
Begin or Update
 Your NIST 800-171 self-assessment.
- 
Identify
 Missing or outdated SSP and POA&M documentation.
- 
Assign Owners
 For control families.

60

 days





IN THE NEXT 60 DAYS

- 
Begin Remediation
 Of audit-sensitive controls.
- 
Build or Refresh
 Policies and repeatable processes.
- 
Establish
 A centralized evidence repository.
- 
Review
 IR, access, and configuration workflows.

90

 days

IN THE NEXT 90 DAYS

- 
Engage a C3PAO
 Or schedule a readiness review.
- 
Complete
 A full internal gap analysis.
- 
Prepare
 For an evidence walkthrough.
- 
Establish
 A recurring compliance cadence.

CMMC readiness is now a competitive differentiator.

Contractors who act early minimize cost, avoid assessment bottlenecks, and protect revenue pipelines. Fortreum's compliance experts are ready to help you interpret your readiness and build your 90-day plan.