KeyStone solutions, llc

CLIENT ADVISORY
June 29, 2026

U.S. DEPARTMENT OF DEFENSE COMPLIANCE

Understanding CMMC: What It Means for Your Business

A new Department of Defense cybersecurity requirement now affects your ability to win and keep defense work. Here is what is changing — and what to do before the November 2026 deadline puts you under pressure.

Why this matters

If your company does any work for the U.S. Department of Defense — as a prime contractor or anywhere in a supplier's chain — **CMMC** (Cybersecurity Maturity Model Certification) now affects your ability to win and keep that work.

It is the DoD's way of confirming that the companies it works with actually protect sensitive information. Starting in late 2026, for many contracts you won't just *promise* you're secure — you'll have to **prove it** through an independent assessment before the contract is awarded.

KEY DEADLINE

Nov 10, 2026

Most contracts involving controlled information will require third-party certification **before award.**

12–18 months to earn certification. **The time to start is now.**

How it phases in

Nov 10, 2025
DFARS rule takes effect — CMMC begins phasing in.

Now • 2026
Begin your gap assessment and build your plan.

Nov 10, 2026
Level 2 third-party certification required for many contracts.

The three levels, in plain terms

Which level applies usually comes down to one question: do you touch CUI?

LEVEL 1

Basic federal contract information

HOW YOU PROVE IT

You assess yourself once a year.

MOST CONTRACTORS

LEVEL 2

Controlled Unclassified Information (CUI)

HOW YOU PROVE IT

An independent, accredited assessor certifies you.

LEVEL 3

Most sensitive information & advanced threats

HOW YOU PROVE IT

The government assesses you directly.

DFARS rule effective Nov 10, 2025; Level 2 third-party certification phasing in Nov 10, 2026. Source: U.S. DoD CIO CMMC program, dodcio.defense.gov/CMMC.

What you should do

1. **Find out if you're affected.**
   Check your DoD contracts and ask your prime contractors whether CMMC is coming. If you handle CUI, assume Level 2.

2. **Get a gap assessment.**
   Know where you stand against the **110 security controls** Level 2 requires. This is the single most useful first step.

3. **Build your plan and paperwork.**
   Certification requires a documented security plan (an SSP) and a remediation plan (a POA&M) for anything not yet in place.

4. **Start early — assessor capacity is limited.**
   There are only so many accredited assessors, and the line is growing. Companies that wait face higher costs and a real risk of missing contract deadlines.

5. **Confirm your IT and cloud can handle CUI.**
   Standard commercial email and tools often aren't enough — you may need a specialized, government-grade environment.

What to watch out for

⚠

One vendor that both fixes and certifies you

That's a prohibited conflict of interest. Readiness help and the assessment must come from separate organizations.

⚠

"Your SOC 2 makes you CMMC-ready"

Be skeptical. Existing certifications help, but they are not the same thing as CMMC.

⚠

"Certified in a few weeks"

Be cautious. Done properly, this is a months-long effort — not a quick stamp.

HOW KEYSTONE HELPS

We help you get ready — and stay ready.

We assess where you stand today, build the security plan and documentation the assessment requires, put the right protections in place, and manage them over time so you stay compliant after you're certified. We work alongside an **independent assessor** for the certification itself — keeping that separation clean is part of doing this correctly.

QUESTIONS?

Reach out to your KeyStone account team — well before the deadline puts you under pressure.

833-4ITTaaS
keystone.solutions