EXOSTAR

PRACTICAL GUIDE

CMMC 2026 What Defense Suppliers Need to Do Now

What defense contractors and subcontractors should prioritize while CMMC is under review — CUI protection, NIST SP 800-171 and readiness.

THE QUESTION HAS CHANGED

Can you demonstrate that your CUI is protected today — and prove it?

What changed — and what did not

The CMMC landscape changed in July 2026; the responsibility to protect CUI did not. If applicable DFARS clauses are in your contracts, you must still implement NIST SP 800-171 — and where Phase I applies, complete the required self-assessment and affirmation.

WHAT CHANGED

Phase II is paused

Phase II would have expanded the number of defense suppliers required to undergo an independent third-party CMMC assessment. That planned expansion is now paused.

The pause applies to assessments, not to CUI.

WHAT REMAINS

Protecting CUI still matters

- Protect CUI
- Understand where CUI lives
- Implement applicable NIST SP 800-171
- Maintain accurate documentation
- Complete applicable self-assessments
- Maintain objective evidence
- Manage remediation
- Prepare for customer or government scrutiny

02 / READINESS DIAGNOSTIC

7 questions every defense supplier should answer

Third-party CMMC assessments may be paused, but organizations still need to understand how CUI is protected and whether they are meeting the cybersecurity requirements in their contracts.

01

Where does our CUI actually live?

Identify the systems, applications, endpoints and collaboration environments where CUI is stored, processed or transmitted.

Email | M365 | Shared drives | File transfer | Endpoints | Supplier portals | Engineering apps | Legacy systems | OT | Third-party platforms

02

Can employees accidentally move CUI outside the controlled environment?

Examine how information moves to customers, primes, suppliers and subcontractors.

Watch for: standard email attachments | personal devices | consumer file-sharing | unmanaged endpoints | unauthorized apps

03

Have we implemented the applicable NIST SP 800-171 requirements?

If applicable DFARS cybersecurity requirements are in your contracts, protecting CUI requires more than having policies on paper.

Understand which NIST SP 800-171 requirements apply and whether the required cybersecurity practices are actually implemented.

04

Can we prove with evidence that controls are working?

Ask what evidence you could show tomorrow for every security requirement.

Configurations | screenshots | logs | policies | procedures | access records | training records | monitoring records

SCOPE PRINCIPLE

If you don't know where CUI travels, it's difficult to know what needs to be protected.

Finish the 7-question test

The last three questions determine whether your documentation and evidence can support your own compliance representations.

05

Does our SSP accurately reflect our environment?

Your System Security Plan should document how your organization protects CUI and implements applicable security requirements.

It should reflect how your environment operates today and be updated as systems, users, processes or CUI workflows change.

06

Are we identifying and actively addressing security gaps?

If a requirement isn't fully implemented, understand the gap and have a plan for addressing it — a Plan of Action and Milestones (POA&M). Unresolved gaps shouldn't disappear into a spreadsheet.

What remains unresolved | who owns remediation | the target completion date | the evidence that will demonstrate remediation

07

Can we confidently support our self-assessment and affirmation?

Where CMMC Phase I self-assessment and affirmation requirements apply, organizations still need to evaluate their cybersecurity implementation and make the required submissions.

Do we have the documentation and objective evidence to support what we're representing about our cybersecurity posture?

A DEFENSIBLE POSITION

The CUI exposure test

Third-party CMMC assessments may be paused, but the cybersecurity requirements in your contracts still matter. Use this quick check to evaluate whether you have the fundamentals in place.

Know your CUI

- [ ] We know where CUI is stored.
- [ ] We know which systems process CUI.
- [ ] We know how CUI is transmitted and shared.
- [ ] We know which employees and third parties can access CUI.
- [ ] We control how CUI is accessed and shared outside our organization.

Protect your CUI

- [ ] We understand the DFARS cybersecurity requirements in our contracts.
- [ ] We have implemented the applicable NIST SP 800-171 requirements.
- [ ] We have appropriate identity, authentication and access controls for CUI.
- [ ] We regularly identify and address cybersecurity gaps.

Document & demonstrate

- [ ] Our SSP accurately reflects our current CUI environment and security practices.
- [ ] Our POA&Ms are current and actively managed.
- [ ] We maintain documentation and objective evidence for each requirement.
- [ ] We can produce supporting evidence when needed.
- [ ] We have the evidence needed for our self-assessment and affirmation.

12–14
CHECKED
You have many of the foundational elements of a defensible cybersecurity program.

8–11
CHECKED
You may have meaningful gaps in documentation, evidence, scope or security implementation.

0–7
CHECKED
Your organization should consider conducting a structured CUI and cybersecurity readiness review.

WHAT THIS IS REALLY ABOUT

The goal isn't simply to be ready for a future third-party assessment. It's to demonstrate that you're protecting CUI and meeting the requirements that apply to your organization today.

04 / SCOPE STRATEGY

Reduce the problem before trying to solve it

One of the biggest CMMC mistakes organizations can make is assuming their entire corporate environment needs to become part of the compliance boundary.

ASK A DIFFERENT QUESTION

Can we reduce where CUI is stored, processed and transmitted?

Corporate environment
Every system, user and device across the business

Systems that touch sensitive workflows
Where CUI is actually created, used and shared

Controlled CUI environment
A boundary you can secure, document and prove

The less CUI spreads, the easier it is to control and protect.

SECURE
Fewer systems and endpoints

MANAGE
Simpler operations

DOCUMENT
Cleaner governance

PROVE
Easier evidence collection

CONTROLLED COLLABORATION ENVIRONMENT

Keeping CUI within a controlled environment can reduce unnecessary exposure and the number of systems, users and workflows that need to be secured and documented.

Build a defensible body of evidence

Protecting CUI isn't just about implementing cybersecurity requirements. Organizations also need to document and support what they've implemented, particularly when completing applicable self-assessments and affirmations.

Maintain a clear body of evidence that connects:

Requirement
What the rule asks

Implementation
How you meet it

Evidence
What proves it

Status
Where it stands

This helps your organization confidently support its compliance position, respond to customer or government questions, and adapt as CMMC requirements evolve.

01 System proof
Configurations, logs, screenshots and technical settings.

02 Governance proof
Policies, procedures, SSP content and POA&M records.

03 People proof
Training records, access records and role assignments.

04 Operations proof
Monitoring records and evidence that practices are followed.

DESIGN PRINCIPLE

If you're affirming that requirements are being met, you should have the documentation and evidence to support that conclusion.

06 / USE THE REVIEW PERIOD

Do not wait for the government review to finish

Organizations that stop cybersecurity work while CMMC is being reconsidered may simply create a larger remediation problem later. Use the review period to strengthen the fundamentals.

A FIVE-PART ACTION FRAMEWORK

01. PROTECT

Secure the systems where CUI is stored, processed and transmitted.

02. REDUCE

Limit unnecessary CUI exposure and shrink the compliance boundary where practicable.

03. DOCUMENT

Keep SSPs, policies, procedures and POA&Ms aligned with actual operations.

04. PROVE

Build objective evidence demonstrating that required security practices are implemented.

05. ADAPT

Track government changes without rebuilding the entire cybersecurity program each time CMMC evolves.

THE TAKEAWAY

Don’t build your cybersecurity program around a future assessment. Build it around protecting CUI today.

Your 30-day CUI protection action plan

Use the next 30 days to strengthen how your organization protects CUI and supports its contractual cybersecurity requirements.

WEEK 1

DISCOVER

- Map where CUI is stored, processed and transmitted
- Identify systems and users with CUI access
- Review external sharing and collaboration

WEEK 2

PROTECT

- Understand the cybersecurity requirements in your contracts
- Review applicable NIST SP 800-171 implementation
- Identify security, documentation and evidence gaps

WEEK 3

REDUCE

- Identify unnecessary CUI locations
- Look for opportunities to isolate CUI
- Strengthen access and external sharing controls

WEEK 4

DOCUMENT & PROVE

- Update your SSP and POA&Ms
- Organize policies, procedures and objective evidence
- Build the evidence repository
- Assign remediation owners
- Confirm you can support the applicable self-assessment and affirmation

30-DAY OUTCOME

Know where your CUI is, protect it appropriately, and have the documentation and evidence to support your compliance.

CMMC may change. Your CUI still needs protection.

The organizations best positioned are those that know where CUI lives, have implemented the appropriate safeguards, and can prove it. Exostar's CMMC Ready Suite™ brings that foundation together — secure CUI collaboration, identity and access management, compliance documentation and evidence management.

WITHOUT A PLAN

- CUI scattered across unmapped systems
- Documentation that drifts from reality
- Evidence assembled under pressure
- Every CMMC change means starting over

WITH CMMC READY SUITE™

- A controlled environment for CUI
- SSPs, POA&Ms and policies kept current
- Objective evidence ready on request
- A foundation that adapts as CMMC evolves

Exostar helps organizations protect CUI today and stay ready for what comes next.