IRONGATE
CYBER DEFENSE SOLUTIONS
TRUST BUILT ON VERIFIED CONTROLS
Powered By Executech

What the current CMMC pause means for your organization

Understanding the temporary delay in CMMC assessments, and why the requirements you are already subject to have not gone anywhere.

WHAT HAS BEEN PAUSED

The Department of War (DoW) is finalizing the implementation of CMMC 2.0 and the associated rulemaking process. As a result, mandatory third-party CMMC assessments (C3PAO) for many contractors have not yet been fully implemented across all contracts.

READ THIS CAREFULLY

This is an administrative delay. It is not a cancellation of the program.

A cancellation would remove the requirement. A delay moves the date and compresses the runway for everyone who waits.

WHAT HAS NOT CHANGED

- ✓ NIST SP 800-171 requirements remain in effect.
- ✓ Contractors handling Controlled Unclassified Information (CUI) are still required to protect that information.
- ✓ Existing DFARS cybersecurity clauses continue to apply.
- ✓ The DoW continues to expect organizations to implement required security controls and maintain appropriate documentation.

IN SHORT Your organization is still responsible for securing its environment and demonstrating compliance. The obligation did not pause. Only the assessment mechanism did.

WHY YOU SHOULD CONTINUE PREPARING

Waiting until CMMC certification becomes mandatory creates real exposure:

- Limited availability of certified assessors once demand spikes
- Increased implementation investment under time pressure
- Compressed remediation timelines
- Delays in bidding on or renewing DoW contracts
- Greater business risk if security gaps are discovered late

Organizations that prepare now will be in a materially stronger position when CMMC requirements begin appearing in contracts.

What your organization should be doing now

The window is open. These are the steps that compound while it stays open.

IMMEDIATE PRIORITIES

1. **Complete a gap assessment**
   Run a CMMC or NIST SP 800-171 gap assessment to establish your actual baseline against the controls.
2. **Develop or update your SSP**
   Your System Security Plan is the document an assessor reads first. It should reflect your environment as it exists.
3. **Create and maintain a POA&M**
   A Plan of Action and Milestones turns your open gaps into a tracked, defensible remediation record.
4. **Remediate identified deficiencies**
   Close the gaps the assessment surfaces, prioritized by risk and by the controls most likely to appear in contract language.
5. **Strengthen core security**
   Harden identity, endpoint, and network security. Implement multi-factor authentication where required.
6. **Build the operating processes**
   Establish incident response and vulnerability management. Improve security awareness training. Review vendor risk.
7. **Prepare your evidence**
   Collect and organize the artifacts a future assessment will require, while the timeline is still yours to control.

HOW EXECUTECH CAN HELP

Assess
CMMC readiness assessments and NIST SP 800-171 gap assessments to establish where you actually stand.

Document
SSP development, POA&M creation and management, policy and procedure development.

Implement
Security control implementation, Microsoft GCC High migrations, and evidence collection.

Sustain
Ongoing compliance management and CMMC assessment preparation, so your posture holds between milestones.

BOTTOM LINE

The current delay should be viewed as an opportunity, not a reason to postpone cybersecurity improvements. Organizations that continue preparing today will be better positioned to achieve compliance, reduce cybersecurity risk, and remain competitive for future Department of War contracts.

> The best time to prepare for CMMC is before it becomes a contractual requirement.

A readiness assessment is the fastest way to know where you stand. Most organizations surface gaps that are inexpensive to close now and expensive to close under a contract deadline. Contact your Executech team or visit executech.com/irongate-cmmc-advisory to start.