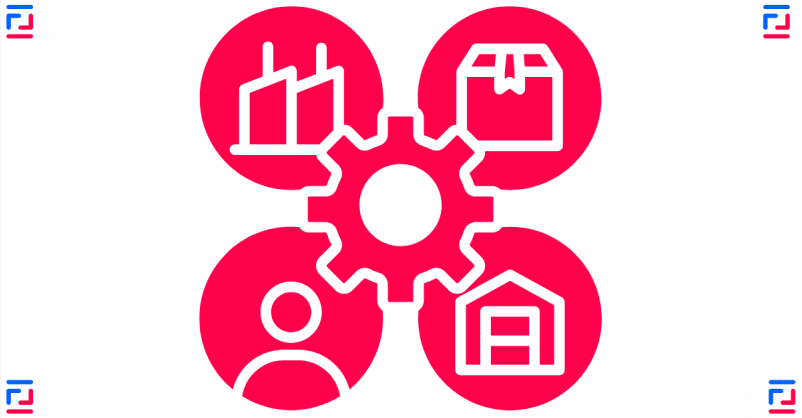
CMMC Nov. 10 Deadline and What It Means for Defense Contractors

STACK Cybersecurity Urges Defense Contractors to Prepare for Nov. 10 CMMC Deadline



Manufacturing cybersecurity

LIVONIA, MI, UNITED STATES, September 10, 2025 / EINPresswire.com/ -- As the U.S. Marine Corps celebrates its 250th anniversary on November 10, the Department of Defense will begin enforcing Cybersecurity Maturity Model Certification (CMMC) 2.0 requirements for all new contracts. STACK Cybersecurity, a Registered Practitioner Organization (RPO) under the CMMC framework, is helping contractors fortify their cyber defenses to meet the new standards before the deadline.

> CMMC isn't just a checkbox. It's a shift in how the government evaluates cyber risk. We're working closely with clients to ensure they're not only compliant but resilient."
>
> *Tracey Birkenhauer, VP of STACK Cybersecurity*

The Cyber AB is the official accreditation body of the CMMC ecosystem and the sole authorized non-governmental partner of the U.S. Department of Defense (DoD) in implementing and overseeing CMMC conformance. Founded in January 2020 as The CMMC Accreditation Body, Inc., The Cyber AB is a Maryland-based, 501(c)(3) organization. The nonprofit supports this security initiative via a direct contract with the CMMC Program Management Office (PMO) in the DoD.

Certified through The Cyber AB, RPOs like STACK Cybersecurity are defined as: "An organization authorized to represent itself as familiar with the basic constructs of the CMMC Standard, with a CMMC-AB provided logo, to deliver non-certified CMMC Consulting Services. Signifies that the organization has agreed to the CMMC-AB Code of Professional Conduct."

The final rule, published for inspection on Sept. 9, amends the Defense Federal Acquisition

Regulation Supplement (DFARS) and launches a three-year phased rollout. By 2028, all defense contracts will require CMMC certification as a condition of award.

After years of development, revisions, and regulatory reviews, the final pieces of the CMMC program are now in place. CMMC requirements can begin appearing in contracts, requests for proposals (RFPs), and requests for information (RFIs) on Nov. 10.

For manufacturers in the defense sector, this shift is particularly significant. Companies handling Controlled Unclassified Information (CUI) will need to implement comprehensive cybersecurity measures aligned with National Institutes of Standards and Technology (NIST) SP 800-171 standards and, in many cases, undergo third-party assessments to verify compliance.

"The requirements apply to components of nonfederal systems that process, store, or transmit CUI or that provide protection for such components," according to NIST.

CMMC RPO Shield

STACK Cyber announces SOC 2 Type 2 certification

Why Cybersecurity Compliance Matters

The defense industrial base (DIB) faces unprecedented cybersecurity threats. Foreign adversaries continuously target defense contractors to steal intellectual property, disrupt supply chains, and access classified projects. For manufacturers producing critical components for military systems, these threats pose risks not only to business operations but to national security.

CMMC Level 2 compliance requires implementation of 110 security controls from NIST SP 800-171, addressing everything from access control and configuration management to incident response and physical security. These controls create a comprehensive security framework

designed to protect sensitive defense information throughout the supply chain.

How STACK Cybersecurity Can Help

As a registered practitioner for CMMC and a company with SOC 2 Type II certification, STACK Cybersecurity is uniquely positioned to guide defense contractors through the compliance process. Our expertise spans both the technical requirements of CMMC and the specific challenges faced by manufacturing companies in the defense sector.

Our team of security specialists understands that compliance isn't just about checking boxes. It's about implementing sustainable security practices that protect your business and your clients.

With our proven methodology, we help clients conduct thorough gap assessments to identify compliance shortfalls, develop comprehensive System Security Plans (SSPs), implement necessary security controls, and prepare for third-party assessments. We also help our clients maintain ongoing compliance. We even price shop to help our clients find the best pricing on assessors. Note we've been quoted from $70,000-$130,000 for a single C3PAO assessment.

For manufacturers handling CUI, the journey to CMMC compliance can be particularly complex. Production environments often involve specialized equipment, legacy systems, and complex supplier relationships that require carefully tailored security approaches. Our manufacturing-specific expertise helps address these unique challenges.

The Time to Act Is Now

With less than two months remaining until CMMC requirements begin appearing in contracts, defense contractors cannot afford to delay their compliance efforts. CMMC Level 2 certification typically takes at least a year, often much longer, depending on a supplier's security posture and its unique level of executive support.

For manufacturers in the defense sector, the process often involves:

1. Identifying where CUI exists within your environment
2. Establishing appropriate boundaries for security implementation
3. Assessing current compliance against NIST 800-171 requirements
4. Developing and implementing remediation plans
5. Creating comprehensive documentation
6. Preparing for assessment
7. Determining whether an enclave is appropriate to reduce scope

CMMC 2.0 includes three certification levels:

Level 1: Self-assessment for contractors handling Federal Contract Information (FCI).
Level 2: Applies to Controlled Unclassified Information (CUI); may require a self-assessment or third-party assessment.

Level 3: Reserved for highly sensitive CUI; requires a government-led assessment.

Contracting officers will verify certification status through the Supplier Performance Risk System (SPRS). Vendors without certification will be ineligible for contracts, task orders, or delivery orders. Conditional certifications will be allowed for Level 2 and Level 3 contractors who submit a Plan of Action and Milestones (POA&M), but these expire after 180 days if full compliance isn't achieved.

What Defense Contractors Need to Know
The implementation will follow a phased approach over the next several years:

Phase 1 (Q4 2025): Beginning Nov. 10, 2025, select contracts will require CMMC Level 2 compliance. During this initial phase, some contractors handling CUI will be allowed to self-assess, while others will need a CMMC Third-Party Assessment Organization (C3PAO)-led assessment.

Phases 2-4: Over the following years, an increasing number of contracts will require CMMC certification, with full implementation expected by 2028.

"With the Pentagon's November 10 deadline fast approaching, contractors must act now to assess their readiness and close any gaps," said Tracey Birkenhauer, VP of Compliance at STACK Cybersecurity. "Our team is here to support them every step of the way."

STACK Cybersecurity continues to expand its advisory services, training programs, and readiness assessments to help clients navigate the evolving landscape of cybersecurity compliance. Not only can STACK Cybersecurity identify any security gaps, we can remediate any technical or cybersecurity issue that exists.

A Dual Celebration: Cybersecurity Milestones and Military Heritage
It's fitting the CMMC implementation date falls on such a significant military anniversary. As the Marine Corps celebrates 250 years of defending American interests on Nov. 10, 2025, the defense industrial base will be embracing a new era of cybersecurity to protect those same interests in the digital domain.

The Marines' 250th birthday represents a milestone of discipline, commitment, and excellence, values that also drive effective cybersecurity programs. Across the country, celebrations will mark this historic occasion, from the recreation of The Tun (the historic tavern where the first Marines were recruited) to the 100th Marine Corps Birthday Ball being held in the same Philadelphia ballroom as the first Ball in 1925.

STACK Remains Ready
At STACK Cybersecurity, we're proud to stand alongside defense contractors in this important transition. As a Registered Provider Organization for CMMC and a SOC 2 Type II certified

company, we bring the expertise and experience needed to navigate the compliance journey successfully.

The countdown has begun. Is your organization ready?

Media Contact:
Tracey Birkenhauer
STACK Cybersecurity
info@stackcybersecurity.com
(734) 744-5300

Tracey Birkenhauer
STACK Cybersecurity
+1 734-744-5300
email us here