BY THOMAS J. DEMAYO, NICK DELENA AND JIM SZUMLASKI | PKF O'CONNOR DAVIES

CMMC COMPLIANCE

A COMPETITIVE IMPERATIVE FOR DEFENSE MANUFACTURERS

Cybersecurity Maturity Model Certification (CMMC) compliance now determines which manufacturers can compete for U.S. Department of Defense (DoD) contracts. To help minimize exposure across the defense supply chain, the DoD requires any business pursuing contract work to demonstrate that it – and its suppliers – have achieved defined levels of effectiveness in internal cybersecurity controls. For many organizations, this means strengthening existing programs. These requirements now apply broadly across the Defense Industrial Base (DIB).

" CMMC establishes required cybersecurity standards for defense contractors and suppliers. Increasingly, it serves not merely as a compliance requirement, but as a qualification threshold for participation in the defense marketplace."

For manufacturers, compliance frequently extends beyond traditional IT environments into plant-floor operations, engineering systems and third-party suppliers supporting production, logistics and quality control. Even companies that consider themselves "indirect" defense suppliers may fall within CMMC scope due to embedded components, technical drawings or controlled unclassified information (CUI) flowing through manufacturing systems.

FROM COMPLIANCE TO QUALIFICATION: UNDERSTANDING THE CMMC FRAMEWORK

CMMC establishes required cybersecurity standards for defense contractors and suppliers. Increasingly, it serves not merely as a compliance requirement, but as a qualification threshold for participation in the defense marketplace.

In manufacturing environments, CMMC requirements often intersect with legacy systems, proprietary production data, CAD/CAM files and operational technology (OT) not originally designed with modern cybersecurity safeguards in mind. Early planning and careful scoping are especially critical for organizations operating long equipment lifecycles or decentralized facilities.

CMMC consists of three levels, each corresponding to increasingly rigorous technical requirements for a prime or subcontractor's cybersecurity safeguards. The program became official on November 10, 2025. It was introduced after Defense Contract Management Agency (DCMA) audits found that only 4 percent of companies in the DIB had implemented DFARS 252.204-7012 by the December 31, 2017 deadline.

LEVEL 1: Satisfied through self-attestation.

LEVEL 2: Requires engagement of an independent CMMC Third-Party Assessment Organization (C3PAO).

LEVEL 3: Can only be certified by the DIB Cybersecurity Assessment Center (DIBCAC), a division of DCMA within the DoD, after obtaining Level 2 certification.

These levels represent specific contractual requirements and serve as benchmarks for businesses pursuing DoD work.

The degree of rigor increases with each level. Level 1 requires implementation of 15 safeguards. Level 2 requires 110 safeguards and 320 underlying assessment objectives. As of November 30, 2025, approximately half of the 1,000 companies that had initiated Level 2 certification had succeeded. Level 3 requires an additional 24 requirements from NIST SP 800-172. Both Levels 2 and 3 require C3PAO certification, which remains valid for three years.

A C3PAO may provide certification services or advisory services — but not both for the same contractor. For example, if PKF O'Connor Davies performs a certification assessment, we cannot consult, conduct gap assessments or assist in drafting remediation plans for that same organization.

These measures are designed to protect CUI. Although CUI falls below the threshold of classification under Executive Order 13526 or the Atomic Energy Act, it is still sensitive technical, operational or security-related information.

Within manufacturing organizations, CUI commonly appears in engineering drawings, technical specifications, bills of materials, testing data and quality documentation shared across internal teams and external suppliers. Identifying where this information is created, stored and transmitted is often one of the most challenging — and frequently overlooked — components of CMMC readiness.

"For manufacturers within the defense supply chain, CMMC compliance is no longer solely a cybersecurity issue. It is a competitive, operational and strategic consideration."

THE IMPLEMENTATION TIMELINE: WHAT CONTRACTORS SHOULD ANTICIPATE

CMMC will be implemented in four phases, two of which are already underway:

PHASE 1 – Began November 10, 2025, the effective date of the 48 CFR Part 204 CMMC acquisition rule. The DoD includes CMMC self-assessment requirements in solicitations as a condition of award.

PHASE 2 – Begins November 10, 2026. In addition to Phase 1 requirements, the DoD intends to include CMMC certification requirements for applicable solicitations and contracts.

PHASE 3 – Begins November 10, 2027. CMMC certification will be required for all DoD solicitations and contracts and as a condition to exercise an option period. This phase includes Level 3 requirements for applicable contractors.

PHASE 4 – Begins November 10, 2028. Full implementation. CMMC program requirements will apply to all solicitations and contracts, including option periods.

WHERE ORGANIZATIONS COMMONLY FALL SHORT

Scoping remains one of the most common areas of failure. The CMMC Level 2 Scoping Guide requires contractors to categorize assets as CUI assets, security protection assets, contractor risk managed assets, specialized assets or out-of-scope assets.

External cloud storage must meet security standards equivalent to those defined by the Federal Risk and Authorization Management Program (FedRAMP) moderate baseline.

Self-assessments constitute formal attestations to the government, and misrepresentation of a score may expose an organization to enforcement under the False Claims Act.

Manufacturers frequently struggle with scoping because production systems, engineering workstations and third-party vendor access are often interconnected in ways that are not fully documented. A single improperly scoped machine or shared network segment can unintentionally bring an entire facility – or multiple facilities – within CMMC scope.

SELECTING THE RIGHT CMMC ADVISOR

Given the operational and regulatory complexity involved, advisor selection is a strategic decision.

Organizations should seek professionals who understand how cybersecurity requirements intersect with manufacturing environments and who can provide executive-level guidance when a full-time Chief Information Security Officer (CISO) is not practical. A virtual CISO (vCISO) model can provide access to dedicated cybersecurity and information privacy specialists, experienced IT operational and compliance professionals and expertise in business continuity, disaster recovery and incident response.

Advisors should also demonstrate experience supporting broader government cybersecurity compliance frameworks, including Risk Management Framework (RMF) and Authorization-to-Operate (ATO) initiatives, as well as National Institute of Standards and Technology (NIST) Special Publication 800-53 program development and implementation for classified and CUI.

Penetration testing capabilities are particularly important for organizations pursuing CMMC Level 3 and certain NIST 800-53 baselines.

In addition, defense contractors benefit from advisors who understand the broader regulatory environment, including Defense Contract Audit Agency (DCAA) expectations and the Federal Acquisition Regulation (FAR), which govern the federal government's procurement process.

As your organization competes for DoD contracts, selecting experienced, multidisciplinary advisors is critical.

For manufacturers within the defense supply chain, CMMC compliance is no longer solely a cybersecurity issue. It is a competitive, operational and strategic consideration. Companies that address these requirements proactively are better positioned to protect intellectual property, maintain customer trust and remain eligible for high-value defense contracts.

Our Cybersecurity and Privacy Advisory team works with defense contractors and manufacturers to navigate CMMC readiness, certification strategy and broader government compliance requirements while maintaining the independence required of a certified assessor.

Nick DeLena,CISSP, CISA, CRISC, CDPSE, CMMC-CCA
Is a Partner at PKF O'Connor Davies.
Cybersecurity and Privacy Advisory

Thomas J. DeMayo, CISSP, CISA, CRISC, CEH, CHFI, CCFE, CMMC-CCA
Is a Partner at PKF O'Connor Davies.
Cybersecurity and Privacy Advisory

Jim Szumlaski, CPA
Is a Partner at PKF O'Connor Davies.
Cybersecurity and Privacy Advisory
Co-Lead, Commercial Manufacturing and Distribution