CMMC Terms & Acronyms

openapproach
DEFENSE COMPLIANCE SERVICES

CMMC compliance comes with a lot of acronyms. This guide translates the most common terms so that anyone technical or not can follow a conversation about defense cybersecurity compliance, assessments, and certification. Terms are grouped by topic, with the full name first and the abbreviation in parentheses.

THE FRAMEWORK & THE RULES

Cybersecurity Maturity Model Certification (CMMC): The Department of Defense/War (DoD/DoW) program that requires contractors to prove they meet a set of cybersecurity standards to obtain and keep contracts. It has three levels of increasing rigor.

32 CFR Part 170: The CMMC "Final Rule" is the federal regulation that makes the program official and enforceable.

Defense Federal Acquisition Regulation Supplement (DFARS): The contract rules that put CMMC and data-protection requirements directly into DoD contracts.

NIST SP 800-171: The set of 110 security requirements that CMMC Level 2 is built on; the baseline set of controls for protecting CUI.

THE INFORMATION BEING PROTECTED

Federal Contract Information (FCI): Non-public information the government provides or is created for a contract. Protecting it is the focus of CMMC Level 1.

Controlled Unclassified Information (CUI): Sensitive government information that is not classified but still requires safeguarding. Protecting it is the focus of CMMC Level 2 and above.

KEY DOCUMENTS YOU'LL HEAR ABOUT

System Security Plan (SSP): The core document of any CMMC effort; it describes exactly how an organization meets each security control.

Data Flow Diagram (DFD): A required diagram showing how FCI and CUI is stored, process, or transmitted through systems, networks, and people. One of the core supporting documents.

Plan of Action & Milestones (POA&M): A document listing security gaps not yet met. A limited set of lower-weighted requirements may be temporarily placed on a POA&M to earn a conditional CMMC status, which must be remediated within 180 days to obtain final certification.

THE PEOPLE & ORGANIZATIONS

Organization Seeking Certification (OSC): A company going through a CMMC assessment.

CMMC Third-Party Assessment Organization (C3PAO): An accredited company authorized to perform official CMMC Level 2 certification assessments.

Defense Industrial Base Cybersecurity Assessment Center (DIBCAC): The government body that assesses C3PAOs, performs Level 3 assessments, and conducts random audits to verify compliance.

CMMC Certified Professional (CCP): An individual credential for people who advise on and support CMMC readiness and may serve on assessment teams.

CMMC Certified Assessor (CCA): A higher credential; CCAs perform official Level 2 assessments through a C3PAO.

Registered Practitioner (RP): An individual authorized to provide CMMC consulting and readiness guidance.

Registered Provider Organization (RPO): A company authorized to provide CMMC consulting and readiness services (but not official assessments).

SYSTEMS, TOOLS & IDENTIFIERS

Supplier Performance Risk System (SPRS): The government system that stores a contractor's assessment score and CMMC status.

Commercial and Government Entity (CAGE) Code: A unique identifier required to do business with the government and to participate in CMMC.

Federal Information Processing Standards (FIPS): Federal encryption standards (FIPS 140-validated) required for CMMC and other higher-level compliance frameworks when CUI is being stored, processed, or transmitted.

ENVIRONMENTS & RELATED COMPLIANCE

Government Community Cloud (GCC / GCC High): Microsoft and other cloud environments built to meet government compliance requirements; used by nearly every organization pursuing CMMC.

Enclave: A separated, secured portion of an environment used to handle FCI/CUI, which narrows the scope of what must be assessed.

Federal Risk and Authorization Management Program (FedRAMP): The program that authorizes cloud services for government use; relevant when selecting compliant cloud providers that store, process, or transmit CUI.

NEED HELP NAVIGATING CMMC? Open Approach is a Registered Provider Organization (RPO) with a CMMC Certified Professional (CCP) and Registered Practitioner (RP) on staff, ready to guide your organization through readiness, scoping, and assessment.