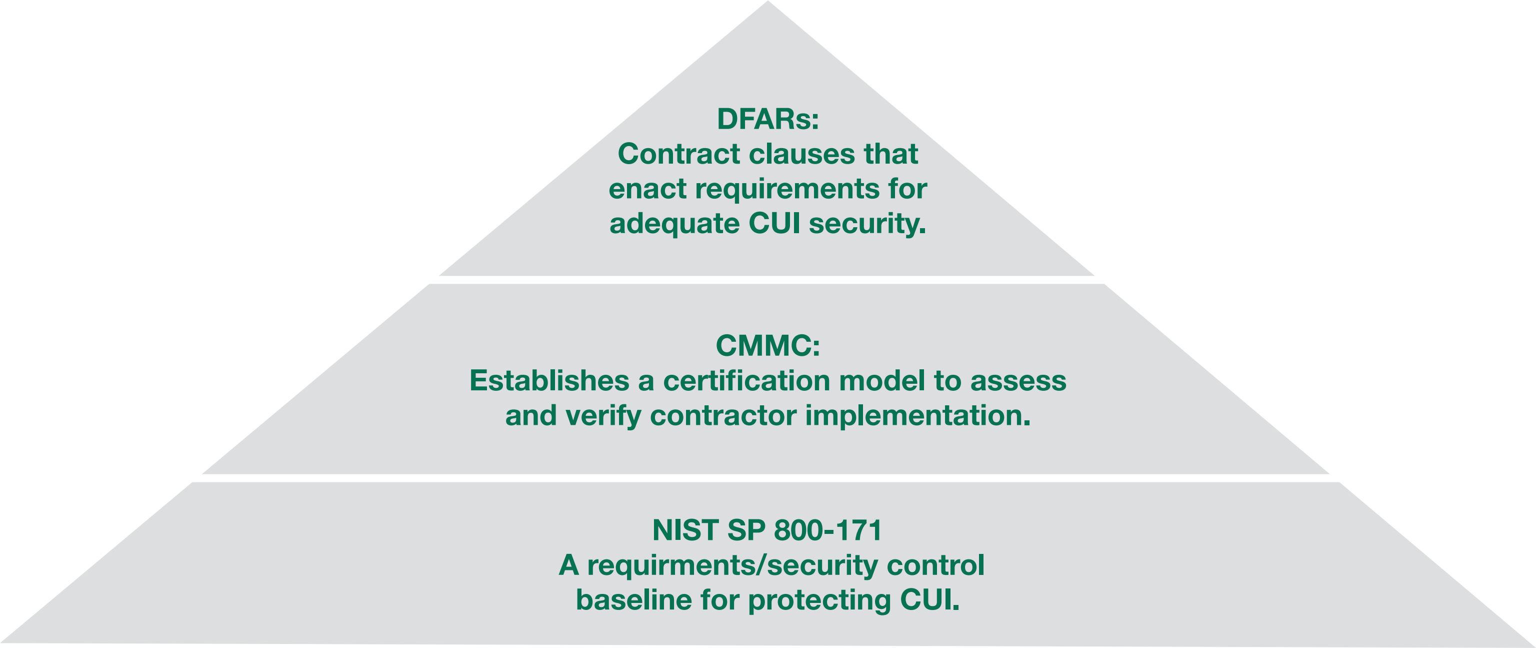
PROTECTING CONTROLLED UNCLASSIFIED INFORMATION (CUI)

The Department of Defense's Final Rule on the Cybersecurity Maturity Model Certification (CMMC) Program went into effect on December 16, 2024. To help you understand its requirements and its relationship to the Defense Federal Acquisition Regulation Supplement (DFARS) and the NIST Special Publication 800-171, this reference document highlights the most pertinent information.



DFARs:
Contract clauses that enact requirements for adequate CUI security.

CMMC:
Establishes a certification model to assess and verify contractor implementation.

NIST SP 800-171
A requirments/security control baseline for protecting CUI.

Defense Federal Acquisition Regulation Supplement (DFARS)

Contract clauses require implementation and assessment of the NIST SP 800-171.

Clause 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.

Requirements:

- “The contractor shall provide adequate security on all covered contractor information systems.” -252.204-7012 (b)
- “… the covered contractor information system **shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations”** -252.204-7012 (b)(i)
- “Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.” -252.204-7012 (c)(1)(ii)

Clause 252.204-7019 Notice of NISTSP 800-171 DoD Assessment Requirements.

Requirements:

- **“In order to be considered for award, if the Offeror is required to implement NIST SP 800–171, the Offeror shall have a current assessment”** -252.204-7019(b)
- The Basic, Medium, and High NIST SP 800–171 **DoD Assessments are described in the NIST SP 800–171 DoD Assessment Methodology...”** -252.204-7019(b)

Procedures:

- “The Offeror shall verify that summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) are posted in the Supplier Performance Risk System (SPRS) () for all covered contractor information systems relevant to the offer.” -252.204-7019(c)(1)

Clause 252.204-7020 NIST SP 800-171DoD Assessment Requirements.

Requirements:

- **“The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800–171 DoD Assessment,** as described in NIST SP 800–171 DoD Assessment Methodology...” -252.204-7020(c)

Cybersecurity Maturity Model Certification (CMMC) Program

Adds a structured maturity certification to assess and ensure contractor readiness and facilitates the assessment process.

Final Rule, Effective 12/16/2024

“With this final rule, DoD establishes the Cybersecurity Maturity Model Certification (CMMC) Program in order to verify contractors have implemented required security measures necessary to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).”

Primary Goals	Transition to Future NIST Requirements
✓ Safeguard sensitive information to enable and protect the warfighter. ✓ Enforce DIB cybersecurity standards to meet evolving threats. ✓ Ensure accountability while minimizing barriers to compliance with DoD requirements. ✓ Perpetuate a collaborative culture of cybersecurity and cyber resilience. ✓ Maintain public trust through high professional and ethical standards.	• **“The DoD cites NIST SP 800-171 R2 in this final rule** for a variety of reasons, including the time needed for industry preparation to implement the requirements and the time needed to prepare the CMMC Ecosystem to perform assessments against subsequent revisions.” • “In May 2024, NIST published SP 800-171 Revision 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, after these comments were received. DoD will issue future amendments to this rule to incorporate the current version at that time.”

CMMC Level and Assessment Requirements

CMMC Status	Source & Number of Security Reqts.	Assessment Reqts.	Plan of Action & Milestones (POA&M) Reqts.	Affirmation Reqts.
Level 1 (Self)	• 15 required by FAR clause 52.204-21	• Conducted by Organization Seeking Assessment (OSA) annually • Results entered into the Supplier Performance Risk System (SPRS)	• Not permitted	• After each assessment • Entered into SPRS
Level 2 (Self)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by OSA every 3 years • Results entered into SPRS • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Entered into SPRS
Level 2 (C3PAO)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by C3PAO every 3 years • Results entered into CMMC Enterprise Mission Assurance Support Service (eMASS) • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Entered into SPRS
Level 3 (DIBCAC)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012 • 24 selected from NIST SP 800-172 Feb2021, as detailed in table 1 to § 170.14(c)(4)	• Pre-requisite CMMC Status of Level 2 (C3PAO) for the same CMMC Assessment Scope, for each Level 3 certification assessment • Conducted by DIBCAC every 3 years • Results entered into CMMC eMASS • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(3) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Level 2 (C3PAO) affirmation must also continue to be completed annually • Entered into SPRS

The NIST Special Publication 800-171

A baseline of controls for protecting CUI.

Key Concepts	Nice to Know
• Directed by DFARS clause 252.204-7012 (b)(i) • “The **requirements apply to components of nonfederal systems that process, store, or transmit CUI,** or that provide security protection for such components.” - NIST SP 800-171r2(1.1) • “Chapter Three describes the **fourteen families of security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations.”** - NIST SP 800-171r2(1.3) • “...to provide federal agencies with recommended security requirements for protecting the confidentiality of CUI” - NIST SP 800-171r2(1.1) • The **requirements recommended for use in this publication are derived from [FIPS 200] and the moderate security control baseline in [SP 800-53] and are based on the CUI regulation [32 CFR 2002].** The requirements and controls have been determined over time to provide the necessary protection for federal information and systems that are covered under [FISMA]. - NIST SP 800-171r2	• “Chapter Two describes the fundamental assumptions and methodology used to develop the security requirements for protecting the confidentiality of CUI; the format and structure of the requirements; and the tailoring criteria applied to the NIST standards and guidelines to obtain the requirements.” - NIST SP 800-171r2(1.3) • “Supporting appendices provide additional information related to the protection of CUI in nonfederal systems and organizations including general references; definitions and terms; acronyms; mapping tables relating security requirements to the security controls in [SP 800-53] and [ISO 27001]; and tailoring actions applied to the moderate security control baseline.” - NIST SP 800-171r2(1.3)

Links to Official Guidance

DFARS

Safeguarding Covered Defense Information and Cyber Incident Reporting - 252.204-7012:
https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

Notice of NISTSP 800-171 DoD Assessment Requirements - 252.204-7019:
https://www.acquisition.gov/dfars/252.204-7019-notice-nistsp-800-171-dod-assessment-requirements.

NIST SP 800-171DoD Assessment Requirements - 252.204-7020:
https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements.

CMMC

Department of Defense Chief Information Officer, About CMMC:
https://dodcio.defense.gov/cmmc/About/

CMMC Final Rule:
https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

NIST SP 800-171

NIST SP 800-171r2:
https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final

NIST SP 800-171 DoD Assessment Methodology:
https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf

NIST Special Publication Subseries Descriptions:
https://www.nist.gov/nist-research-library/nist-special-publication-subseries-descriptions

Need help conducting a Self-Assessment or creating a System Security Plan?

Visit **cadre.net/contact-us**