COGR

Advancing Effective Research Policy

Department of Defense Cybersecurity Maturity Model Certification 2.0 Effective December 16, 2024

The Cybersecurity Maturity Model Certification (CMMC) 2.0 is a revised set of cybersecurity standards issued by the U.S. Department of Defense (DoD) that ensures that DoD contractors protect sensitive data appropriately. The CMMC framework is relevant for defense contractors and subcontractors, including universities performing research under a DoD contract, who have access to or are creating Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) during the performance of the contract.

Research that meets the fundamental research criteria will generally not be subject to the CMMC framework. Universities need to note, however, in response to comments, DoD states in the Final Rule that "(w)hen the DoD does determine that research meets the definition of CUI, safeguarding requirements of DFARS clause 252.204– 7012 will apply regardless of whether the contractor's work is fundamental research."

Key Updates in CMMC 2.0:

CMMC 2.0 is intended to make compliance easier for DoD contractors and subcontractors by simplifying the framework in the following ways:

1. **Reduction of Levels**: CMMC 2.0 reduces the number of certification levels from five to three:
    - **Level 1 (Foundational)**: Basic cyber hygiene, applicable for contractors handling FCI.
    - **Level 2 (Advanced)**: Aligns with National Institute of Standards and Technology (NIST) SP 800-171r2 controls, applicable for handling CUI.
    - **Level 3 (Expert)**: Advanced cybersecurity practices for institutions handling more sensitive data.

2. **Self-Assessment and Third-Party Assessments:** CMMC 1.0 required third-party assessment starting at Level 1. CMMC 2.0 allows for self-assessment for Level 1 and, in some cases, Level 2.
3. **NIST SP 800-171 Alignment**: CMMC 2.0 closely aligns with NIST SP 800-171r2 standards for protecting CUI. Universities must ensure compliance with these practices, which include access controls, incident response, configuration management, and more.

Feature	CMMC 1.0	CMMC 2.0
Levels	1. Basic 2. Intermediate 3. Good 4. Proactive 5. Advanced	1. Foundational 2. Advanced 3. Expert
Assessment	Level 1: Third-party assessment Level 2: N/A Level 3: Third-party assessment Level 4: N/A Level 5: Third-party assessment	Level 1: Annual self-assessment Level 2: Triennial third-party assessment for critical national security information, annual self-assessment for other information Level 3: Triennial government-led assessment
Process vs Practice[1]	Focused on practices and processes	Focuses on practices (controls)
NIST Alignment	Not explicitly tied to NIST SP 800-171	Directly aligned with NIST SP 800-171 and a subset of NIST SP 800-172

Steps for Compliance:

1. **Identify CUI or FCI**: Determine whether your institution will create or handle CUI or FCI under the contract (or subcontract). If so, assess what data and systems are involved.

[1] "Practice" refers to a specific technical activity or control needed to achieve a level of cybersecurity. "Process" describes the procedure or methodology used to execute a practice.

2. **Assess Current Practices**: Review existing cybersecurity measures and identify gaps in compliance with NIST SP 800-171 and NIST SP 800-172 (as applicable).
3. **Implement Changes**: Implement technical and administrative safeguards to comply with the appropriate CMMC level.
4. **Prepare for Certification**: As applicable, conduct internal self-assessments or arrange for third-party assessments.

   Self-assessments can be submitted on behalf of an institution through the Supplier Performance Risk System (SPRS) for authorized users associated with an organization's CAGE code. While full reassessments occur every three years, affirmations of the self-assessment must occur annually to avoid a lapse in the assessment.

   - Instructions for user enrollment
   - Instructions for assessment submission

   Third-party assessments must be performed by a CMMC certified third party assessor (C3PAO) or Defense Contract Management Agency (DCMA), depending on the prescribed CMMC level.

   - Information on C3PAO accreditation body and candidate assessors

Scoping of CMMC Levels:

1. **Level 1**: As detailed in §170.19(b), consists of all assets that process, store, or transmit FCI. (CMMC Level 1 Scoping Guide)
2. **Level 2**: As detailed in §170.19(c), consists of all assets that process, store, or transmit CUI, and all assets that provide security protection for these assets. (CMMC Level 2 Scoping Guide)
3. **Level 3**: As detailed in §170.19(d), consists of all assets that can (whether intended to or not) or do process, store, or transmit CUI, and all assets that provide security protection for these assets. The CMMC Level 3 Assessment Scope also includes all Specialized Assets[2] but allows an intermediary device to provide the capability for the Specialized Asset to

[2] Assets that may or may not process, store, or transmit CUI such as government property, Internet of Things devices, and test equipment.

meet one or more CMMC security requirements, as needed. (CMMC Level 3 Scoping Guide)

Phased Implementation of CMMC:

DoD will implement CMMC requirements in four phases over a three-year period. This approach is anticipated to allow ample time for organizations to implement assessment requirements and for CMMC assessors to be trained. The Final Rule is effective December 16, 2024. Implementation Phases are based on the Effective Date.

1. **Phase One**: Commences on the Effective Date. As applicable, DoD solicitations will require Level 1 or Level 2 self-assessments during this phase.
2. **Phase Two**: Begins 12 months after the start of Phase One. In addition to Phase One requirements, solicitations will require Level 2 certification, as applicable.
3. **Phase Three**: Begins 24 months after the start of Phase One. Level 3 certification will be added to solicitation requirements, as applicable.
4. **Phase Four**: Thirty-six months after the start of Phase One, all solicitations and contracts will include appropriate CMMC Level requirements as a condition of contract award.

Cost of CMMC Compliance:

An organization's cost of compliance can vary widely based on a host of factors, including:

- Need to review and update the organization's cybersecurity policies
- Need to hire and/or train staff
- IT equipment needs
- CMMC compliance level required in the solicitation or terms of the contract
- Size and complexity of the organization's IT infrastructure
- Effort required to prepare for an assessment and any remediation activities needed

- Cost of the C3PAO. The overall cost will vary based on the entity contracted to perform the third-party assessment, the time needed for the assessment, and any additional services (i.e., gap analysis, consulting during remediation, and post-assessment support)

It is important to budget for any costs associated with periodic re-assessments and certifications.

DCIO CMMC Resources:

DoD Chief Information Officer maintains useful resources and documentation to assist in compliance with CMMC 2.0 requirements.

- About CMMC
- CMMC Resources and Documentation
- Frequently Asked Questions

For any questions regarding this guidance, please contact Kevin Wozniak, COGR's Director of Research Security & Intellectual Property at kwozniak@cogr.edu.