**Cybersecurity Maturity Model Certification (CMMC)**

The Cybersecurity Maturity Model Certification (CMMC) program is aligned to the Department of Defense (DoD) information security requirements for its Defense Industrial Base (DIB) partners. It is designed to enforce protection of sensitive unclassified information that is shared by the Department with its contractors and subcontractors. The program provides the DoD increased assurance that contractors and subcontractors are meeting the cybersecurity requirements that apply to acquisition programs and systems that process Controlled Unclassified Information (CUI) and/or Federal Contract Information (FCI).

The changes reflected in CMMC 2.0 will be implemented through the rulemaking process. Companies will be required to comply once the forthcoming rules go into effect. DoD intends to pursue rulemaking both in Part 32 of the Code of Federal Regulations (CFR) as well as in the Defense Federal Acquisition Regulation Supplement (DFARS) in Part 48 of the CFR. Both rules will have a public comment period.

On December 26, 2023, DoD published for comment the proposed Part 32 rule for the Cybersecurity Maturity Model Certification (CMMC) 2.0 program at <https://www.federalregister.gov/documents/2023/12/26/2023-27280/cybersecurity-maturity-model-certification-cmmc-program>. Stakeholder input is critical to meeting the objectives of the CMMC program. The public comment period for the Part 32 rule in the CFR closes on February 26, 2024. The Part 48 CMMC DFARS rule is currently undergoing the rule making process.

DoD encourages contractors to continue to enhance their cybersecurity posture during the interim period while the rulemaking is underway. DoD has developed Project Spectrum (<https://www.projectspectrum.io/>) to help DIB companies assess their cyber readiness and begin adopting sound cybersecurity practices.

Additional information on the CMMC program can be found on the DoD Chief Information Officer (CIO) website: <https://dodcio.defense.gov/CMMC/About/>