KEEP DEPARTMENT OF DEFENSE **CONTRACTS COMING**

Gear Up for CMMC Compliance

What's Expected of You

DoD contractors must conduct and deliver a self-assessment of compliance toward NIST Special Publication 800-171's 110 cybersecurity controls.

The self-assessment should result in a score the defense contractors must upload to the federal Supplier Performance Risk System (SPRS) database.

After self-assessment delivery, defense contractors must be prepared for DoD auditing.

Ongoing, comprehensive network scans must be routinely conducted and documented to validate that your security efforts are fully implemented at all times.

In 2025, when CMMC is fully rolled out, compliance will likely intensify. A qualified managed service provider (MSP) can help your organization navigate CMMC complexities.

The U.S. Department of Defense (DoD) has introduced CMMC — the Cybersecurity Maturity Model Certification — to independently audit and certify the cybersecurity of over 300,000 defense contractors.

Until CMMC is fully rolled out in October 2025, the DFARS Interim Rule now requires you to conduct a self-assessment of your implementation of NIST Special Publication 800-171's 110 cybersecurity controls and upload your score to the federal Supplier Performance Risk System (SPRS) database to qualify for new contracts and renewals.

The First Step Towards CMMC Certification

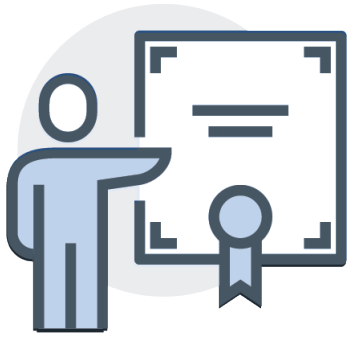
Once you post a score, you will be subjected to an audit by the DoD and will be required to consistently implement cybersecurity best practices and have accurate documentation available for auditing.

Because CMMC is built on the current requirements for NIST 800-171 implementation, your efforts to comply with the Interim Rule will now put you on a direct path to CMMC certification.

RESTECH SOLUTIONS

CMMC - NOT **'ONE-SIZE-FITS-ALL'**

CMMC was designed to secure and improve the integrity of three types of data — Federal Contract Information (FCI), Controlled Unclassified Information (CUI) and Covered Defense Information (CDI) — stored on the information systems of federal contractors and their supply chain.



Depending on the type of data you process or store, the requirements of the DoD and your prime contractors, you will need to be prepared for CMMC certification level at one of its five levels. Once certified, you will be qualified to be awarded contracts at all levels up to your certification.

CMMC Levels 1-5

CMMC Level 1 protects general contract information if you do not store or process CUI or CDI. Because the DoD contracts with many businesses for general supplies and services, it is estimated that 50% to 60% of defense contractors will just have to implement the 17 cybersecurity controls defined in CMMC Level 1.

If you do store or process CUI or CDI, you will need to be certified for CMMC Level 3's 130 cybersecurity controls made up of the 110 controls in NIST SP 800-171 plus 20 additional controls. It is estimated that only a very small percentage of contractors will be required to be certified at Levels 4 or 5.

RESTECH SOLUTIONS

THE INTERIM RULE AND **ASSESSMENT READINESS**

Because CMMC is expected to be rolled out over five years, the DFARS Interim Rule began requiring defense contractors to perform self-assessments of their cybersecurity using the NIST 800-171 DoD Assessment Methodology as of November 30, 2020. If you don't post a score, you will not be eligible for new contracts or renewals.

The unusual scoring methodology starts out at a perfect score of 110 points (based on 110 controls in NIST SP 800-171), after which you deduct 1 to 5 points for missing controls. Depending on what controls you have not fully implemented, it is possible to have a negative score.

Planning for Future Control Implementation

You must upload your score to SPRS and have a written System Security Plan (SSP) documenting your network and identifying all the controls you have fully implemented. For all controls not fully implemented, you must have a written Plan of Action & Milestones (POA&M) identifying each missing control, what you are doing to implement it and the target date.

Move Towards Certification

Start your journey towards CMMC certification by completing and implementing the self-assessment that is due right now. We have the tools and experience to measure your cybersecurity controls and help you achieve a perfect score.

Let us help you prove compliance with NIST Special Publication 800-171's 110 cybersecurity controls now and prepare for future CMMC goals.

RESTECH SOLUTIONS

Contact us today to start your journey towards CMMC Compliance!