

Everything You Need to Know About the CMMC

By Sese Bennett



PROVINCIA
GOVERNMENT SOLUTIONS

Everything You Need to Know About the CMMC

By Sese Bennett

CMMC is the latest development in the Cybersecurity Maturity Model Certification (CMMC), recently announced by the Department of Defense (DoD). The CMMC will affect every DoD contractor along the supply chain and will include any DoD contractor regardless of the type of information handled. As such, the pressure is on for contractors to fully understand the new CMMC guidelines and be prepared to comply with them.


We're providing insight into the CMMC to help contractors understand the new regulations and prepare for the new certifications.

What is the CMMC?

The CMMC refers to the Cybersecurity Maturity Model Certification that will replace the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 assessment model currently in place for contractors of the DoD.



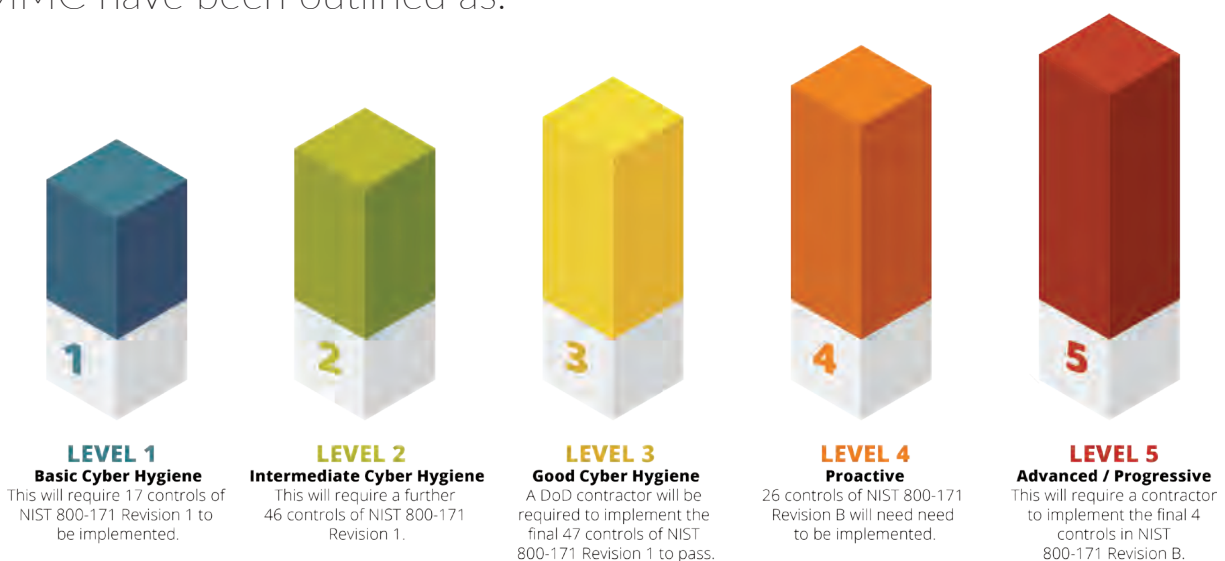
This new certification will require third party evaluation in order to determine whether a contractor is secure enough to work with the DoD. The CMMC aims to ensure that all contractors dealing with the DoD are able to protect the Controlled Unclassified Information (CUI) that they may be handling in their work.



The CMMC will be a unified cybersecurity standard for DOD acquisitions which will boost the cybersecurity posture of the Defense Industrial Base (DIB). The certification focuses on various cybersecurity standards and best practices that range from basic cyber hygiene to the more advanced cybersecurity controls.

To gain a CMMC certification, a contractor will need to understand the associated practices that when implemented, will reduce risk against a specific set of cyber threats. The CMMC is intended to be cost-effective and affordable for small businesses to implement at the lower CMMC levels. Certified independent 3rd party organizations will conduct audits and inform risk, depending on the kinds of data a contractor is handling.

Most of the information that has been released on the CMMC is provisional and has been released by [The Office of the Under Secretary of Defense for Acquisition and Sustainment](#). They are set to release a final version (Rev 1.0) in January 2020 with another version that includes Requests for Proposals in June 2020. The levels of the CMMC have been outlined as:



Why CMMC Now?

In recent years the DoD has experienced a high profile set of data breaches that have put public information at risk. As such, the DoD has been forced to take a look at the security controls surrounding every contractor who works with them. At the time of these breaches, the DoD were reliant on the NIST SP 800-171 as their guidelines.

As the compromise of sensitive data has occurred in the contractor supply chain, the DoD have tightened controls on CUI in this area. The DoD understand that the leakage of this Controlled Unclassified Information could have catastrophic results, and therefore they are putting security at the top of their priority list. While traditional procurement models will stay in place, security will be seriously considered alongside cost, delivery timeline and quality of output in order to protect the DoD from further security breaches.



CMMC Building Blocks

The CMMC will be a unified cybersecurity standard for DOD acquisitions. The standard combines various cybersecurity standards and best practices, which are mapped across several maturity levels.

The CMMC builds on a variety of security standards and best practices including but not limited to:

- [DFARS 252.204-7012](#)
- [NIST SP 800-171](#)
- [NIST SP 800-171B](#)
- [NIST SP 800-53](#)
- [AIA NAS9933](#)
- [ISO 270001](#)
- [ISO 27032](#)



Who Does it Apply to?

Any contractor doing business with the DoD will need to comply with these standards, including subcontractors. The focus of the CMMC is on supply chain integrity, therefore all suppliers involved in work with the DoD will need to complete the required level of certification. This will go beyond the first tier of supply chain subcontractors to completely open up the supply chain and ensure that anyone working with sensitive data will be certified.

The CMMC was created with this in mind, therefore efforts are being made to ensure smaller companies and subcontractors will still be able to comply.

The varying degrees of compliance depend on the amount of DoD CUI the company handles and not by size. While this may benefit bigger companies, who deal with the same level of CUI as smaller contractors, the DoD is committed to ensuring that small businesses will have equal opportunity to compliance.

Prepare Now for the CMMC

Since the CMMC is building on many previous cybersecurity requirements and guidelines, it will benefit contractors to brush up on their knowledge on past security guidelines. This is especially true of the NIST SP 800-171, since the DoD is building on this heavily to create the CMMC. Although nothing has been confirmed where the maturity levels are concerned, it is thought that implementing and understanding the NIST SP 800-171 will help contractors prepare for the CMMC. Furthermore, it will benefit contractors to meet the existing requirements around Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 concerning safeguarding information and reporting incidents.



Advanced preparation now is essential for successfully navigating the new CMMC program. Performing targeted risk assessments on programs and systems that handle CUI data will enable you to identify possible problem areas where security can be increased.

Remember, the varying degrees of compliance depend on the amount of DoD CUI the company handles and not by size. Proper documentation and implementation of key security programs such as access control, change management, and incident response should detail how you handle CUI and what you would do in the event of a cybersecurity incident involving DoD CUI. These steps will enable a smooth transition to the CMMC.

Using NIST SP 800-171 as a guideline to perform your assessment will increase the likelihood that you are heading in the right direction. If you are unfamiliar with the NIST 800-171 standards or would like to discuss where to start with the CMMC, Provincia Government Solutions is here to help. With over 15 years of government experience including direct experience working with NIST SP 800-171, NIST SP 800-53, FISMA, MARS-E and a host of other government security and compliance regulations, we are well positioned to assist you through this new process.

Provincia Government Solutions is an SBA certified HUBZone and small business. For more information about the CMMC or any of our other services, please contact us at (615) 807-2822, via email at jhoffman@provincia.io, or via our website at <https://provincia.io>.

References

- ACQ
- SysArc.com
- FCW
- ComplyUp.com
- CHIPS Magazine
- Inside Government Contracts