We Need to Go That Way!

Staying Competitive with Cybersecurity Maturity Model Certification Requirements

Robert J Hanley
Vice President-Cyber Solutions and Engineering
Sabre Systems, Inc.

ABSTRACT

The Cybersecurity Maturity Model Certification (CMMC). What is it? Why do you care? This article discusses what you need to know about CMMC and how it will affect you when competing for future contracts. DoD did not consider self-certification of NIST a success, so the more formal CMMC was created and released in January 2020 to address this problem. If you are a part of the Defense Industrial Base (DIB), you will soon need to attain the appropriate level of CMMC certification. There are three levels, with level 3 being the most stringent.

For most DIB contractors, the target should be Level 3 since this level is the minimum required for anyone handling Controlled Unclassified Information (CUI). CUI encompasses “For Official Use Only” (FOUO), “Sensitive But Unclassified” (SBU), “Law Enforcement Sensitive” (LES) and “Limited Distribution” (LimDis). By late 2020, new Requests for Proposals (RFP’s) will begin requiring cybersecurity certification. DOD expects to fully implement CMMC on new contracts (but not existing contracts) by 2026.

The RFP will define the minimum acceptable CMMC level to compete and additional bonus points will be added to a contractors rating for exceeding the minimum level. Under CMMC, DIB contractors cannot self-certify, so you will have to hire an independent auditor. Every DIB contractor needs to begin to “Go That Way”, that way being to get CMMC certified so you can stay in the game and compete for future DoD contracts. Do not be left behind!

THE CHALLENGE

There are currently about 65,000 defense contractors and sub-contractors. This number grows to over 300,000 when you include vendors. In a 2018 survey of these contractors, nearly 45% indicated they had not even read the NIST 800-171 requirements and less than 1% were self-certified. It has become obvious that how we protect sensitive data was going to have to change from voluntary to mandatory.

The unchecked flow of CUI (or CUI not marked as CUI!) over the internet continues to expand and critical technologies are, or already have been, compromised. As an example, leveraging large amounts of data published in open source and available on the internet, China was able to build their first large aircraft carrier that mirrors U. S. technology (Figure 1).

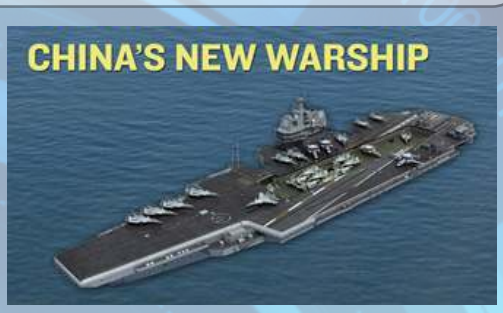

Figure 1: Chinese Aircraft Carrier and Aircraft Modeled after U.S. Technology

In addition, China has built Tactical Aircraft similar to the F-35 also based on open source data. In reality, most of these data should have been marked as CUI, but identifying what is CUI and what is not is also a challenge! The CUI data that is in open source has compromised the United States edge in technology. We have to stop the bleeding and CMMC will help in this endeavor. CMMC lays that framework out.

Another challenge is to have CMMC embraced by all in the DIB and enculturate it across the industry. Of course, making it a part of the requirements set forth in an RFP will help expedite the process, but everyone in the DIB needs to want to do this expeditiously to protect our national intellectual property. Think about it. Even if CMMC was not a requirement, what would happen to your company if it wa s determined that a CUI breach occurred through your negligence? What if you were to lose your Intellectual Property because you failed to apply basic security controls? You will almost certainly lose your reputation, a lot of money and possibly your business altogether (60% of all small businesses go out of business within 6 months after a security breach). By the end of 2020, CMMC will have taken root across the DIB and it is up to all of us to make it a success, not only for National Security but also for your protection!

WHAT LEVEL DO I NEED TO BE CERTIFIED AT FOR CMMC

Every company needs to determine where they will fall under CMMC requirements. There is a lot of guidance online. Sabre Systems provides consultation, CMMC self-assessments and auditing for CMMC customers as well. So, begin that process of "Going That Way" now. Many sub-contractors will fall under level 1 or level 2. Most Prime contractors within the DIB will need at least CMMC level 3 since they all handle CUI. Level 3 provides "good" cyber hygiene, which includes "managed processes." There are costs for a company to attain level 3 or above since this will necessitate dedicated staff to implement and maintain the certification.

Prime contractors will also be responsible for ensuring that their sub-contractors are certified when bidding on an RFP (most sub-contractors should already be ready for a level 1 or 2 certification based on documenting that they meet FAR 52.204-21.) clear how that will be implemented. . Figure 2 highlights the basic requirements and expectations for CMMC.

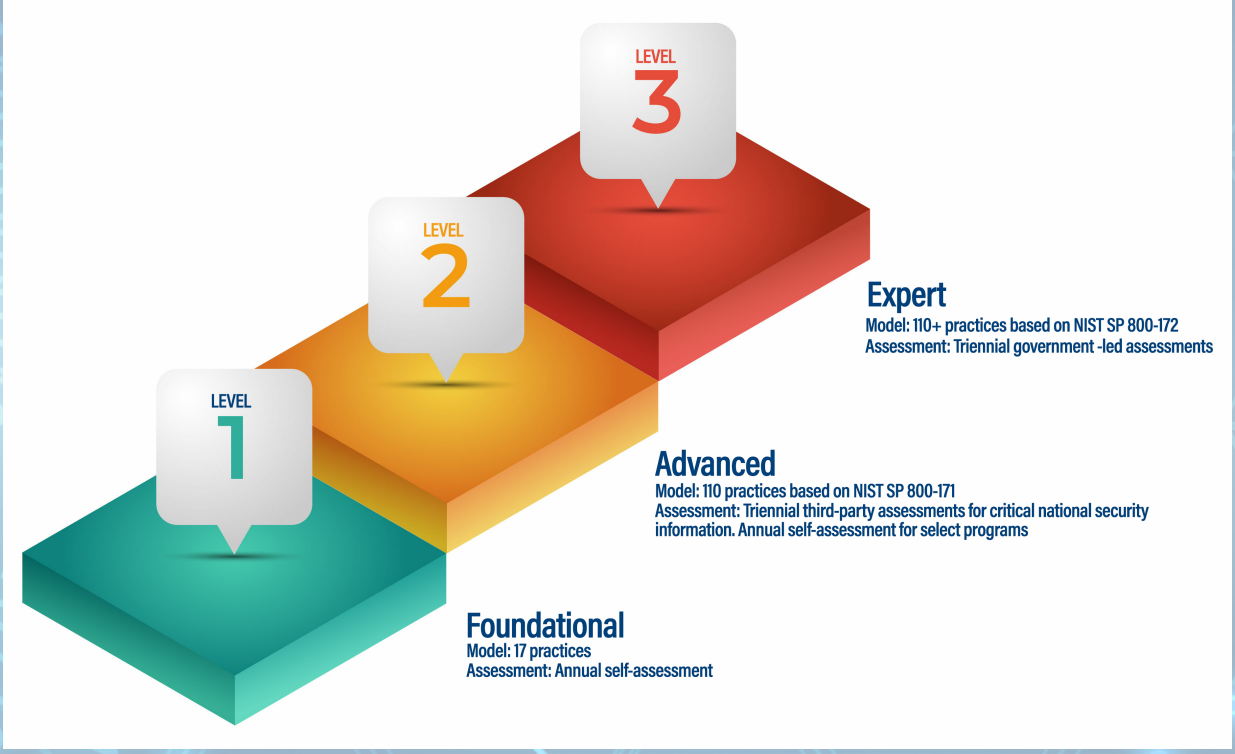

Figure 2: The CMMC Benchmarks for the Three Levels

GETTING STARTED FOR CMMC

Get started now! Get ready for the audit and get certified. Perform a self-assessment. Address and remediate deficiencies. Hire an approved DoD auditor. Execute the audit. Resolve any additional deficiencies. Get certified. You will need to ensure that you have compliant platforms, encrypted assets, data backup and recovery and monitored and managed solutions (for level 3 and above). Do not put this off and have an RFP released that you can no longer bid on because you do not have the proper CMMC level certification!

CONCLUSION

CMMC is here to stay. It is not voluntary. However, you can voluntarily make yourself non-competitive on future DoD contracts if you choose to ignore the requirements. Do not go this way. Get started, get audited, get certified and compete. Go THAT way! Not just because it is a requirement, but also because we all want to protect our technology, our data, our intellectual property and our Nation.

GET STARTED TODAY!

Contact Sabre On Point to learn more.

1-833-337-6468

sabreonpoint.com

Sabre On Point