corsica
technologies

CMMC CHEAT SHEET

What is it?

In 2015, the Department of Defense published "DFARS" which mandated that private DoD contractors adopt cybersecurity standards according to the NIST 800-171 cybersecurity framework. This is part of a government led effort to protect the US Defense supply chain from foreign and domestic cyber threats. Frustrated with slow adoption and, in some cases, false claims regarding compliance from suppliers, the DoD has released the Cybersecurity Maturity Model Certification (CMMC) to ensure appropriate levels of cybersecurity controls and processes are in place to protect contractor systems. The CMMC will encompass multiple maturity levels that range from "Basic Cybersecurity Hygiene" to "Advanced." The intent is to identify the required CMMC level in the RFP and use it as a "go/no go" decision when evaluating vendors.

What does this mean?

There are approximately 300,000 vendors that are subject to CMMC. The DoD estimates that only 10% meet the standard as released. (The official version was released on January 31, 2020.) The DoD plans to release around 20 RFPs this year that will require CMMC when the contract is awarded. By FY26, all new DOD contracts will contain CMMC requirements. All DoD contractors should already be at Level 1 as that parallels some existing requirements. Level 3 is going to be the level that most contractors need to achieve to be relevant.

This sounds hard.

Yes, there is no silver bullet. Meeting the requirements of CMMC requires the integration of multiple solutions. Most of these contractors do not have a "Cybersecurity" expense line on their P&L, so this is a new, and significant, expense for them to consider. An additional challenge is that this is a "pre-award" requirement, meaning that you must demonstrate that you are certified prior to the final award. Previous standards allowed companies to identify the areas of needed improvement and put them on a POAM (Plan of Action and Milestones) to address later.

What are companies doing in response?

The first thing they are doing is getting an assessment. This assessment shows their performance against the standard and the gaps they must fill. A plan of action is then created to address those gaps. For a company that lives and dies by DoD contracts, they have no choice but to comply. One thing we are thinking is that there will be some consolidation in the space. If you make a widget and 10-15% of your revenue is with the DoD, some of those companies are looking to sell that IP and the associated manufacturing processes to another larger, already CMMC certified, company rather than take on that compliance expense for a small revenue stream.

What are the levels and what do they mean?

CMMC Level	Desired Result	Details
Level 1	Basic Cyber Hygiene	17 controls NIST 800-171 rev1
Level 2	Intermediate Cyber Hygiene	48 controls of NIST 800 800-171 rev 1 plus 7 other new controls
Level 3	Good Cyber Hygiene	Final 45 controls of NIST 800-171 rev 1 (110 NIST controls total) plus 14 other new controls.
Level 4	Proactive	13 controls of NIST 800-171 revB plus 13 other new controls
Level 5	Advanced/Progressive	All controls, the remaining 5, of NIST 800-171 revB plus 11 other new controls.

What if my company does this kind of work?

First, you need to get an assessment, soon, to see if there are gaps in compliance and identify what the work effort to become compliant looks like. Then, you are going to look at the cost to become compliant and compare it to the revenue opportunities. If your company does a lot of this kind of work, there will be new, likely unbudgeted, costs put on the organization to simply continue doing what they have been doing. While this is likely already on your radar, the time to act is now since the final standard went live last month.

Can we do this ourselves?

There is a provision for self-audit, but experts do not believe that is wise. The cocktail of services you need to check all the boxes is really complicated to source and manage on your own. Finding a good partner that can provide critical components "as a service" is essential to moving towards compliance in a timely manner.

What do I look for in a partner?

Find a partner that has a team dedicated to cybersecurity. Security is constantly changing and having a team of dedicated specialists with certifications in the security space can provide the peace of mind needed.

Discover the difference of forward-thinking IT.

information@corsicatech.com 877.659.2261 corsicatech.com

corsica technologies

Leadership | Commitment | Experience