River Run's Manufacturers & Government Contractors Guide to CMMC 2.0

Strategic insight on the Department of Defense's Cybersecurity Maturity Model Certification and how it could impact your business

Overview

The U.S. Department of Defense's Cybersecurity Maturity Model Certification (CMMC) and the compliance challenges it presents are perhaps the hottest topics in government contracting right now. In this overview, River Run, a leader in IT and Cybersecurity services and consulting for manufacturers and government contractors, looks at the rationale behind CMMC, where it stands today as CMMC 2.0, and the potentially far-reaching implications for entities that do business with the DoD.

Why CMMC and Why Now?

The Department of Defense (DoD) is deeply concerned about cybersecurity and has made protecting the DoD supply chain from cyberattack a top priority. The agency believes the traditional measures of contractor performance — cost, schedule, and quality — are only effective and applicable in a secure environment. Through the CMMC framework, the DoD is telling defense contractors that security is paramount, and they must meet certain cybersecurity standards in order to work for the DoD in the future.

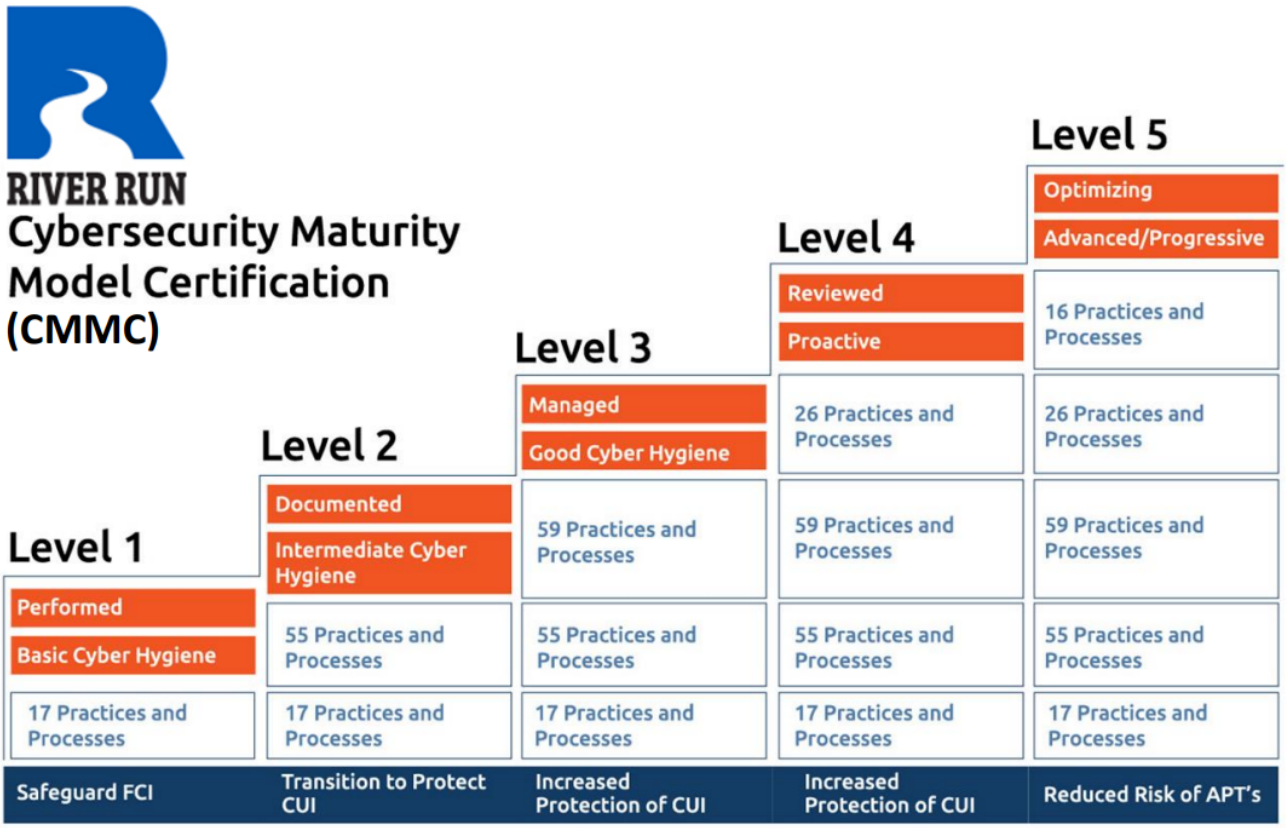
CMMC 1.0 was the next step in an iterative process that began several years ago. To address the need for improved cybersecurity amid increasingly insidious threats, the DoD directed the Defense Industrial Base of government contractors to adopt stronger cybersecurity practices in the form of the NIST 800-171 standard, giving them a target date of December 31, 2017, to come into full compliance with the standard. Compliance was to be based on a self-assessment by each contractor itself. The standard lacked any mechanism for third-party validation of the contractor's self-assessment, as well as any way to track how a contractor was responding to areas of concern identified in its System Security Plan. The December 2017 deadline passed with only partial adoption among the Defense Industrial Base and a very uncertain compliance status.

The limited success of the NIST 800-171 cyber initiative prompted the DoD to seek another way to ensure an appropriate level of cybersecurity and document contractor status in a manner readily visible to contracting officers. The resulting Cybersecurity Maturity Model Certification unveiled by the DoD in 2019 provided a new compliance framework for cybersecurity for DoD acquisitions. The model is similar to management maturity models used by other entities inside and outside the government, with five levels that describe the maturity of a government contractor's cybersecurity practices and processes. Version 1.02 of CMMC was released on December 20, 2020.

In sharing her thoughts on the genesis of CMMC 1.0, Katie Arrington, Chief Information Security Officer (CISO) for the Assistant Secretary for Defense Acquisition, said, "The U.S. is losing $600 billion a year to our adversaries in exfiltration, data theft and R&D loss. If we were able to institute good cyber hygiene and we were able to reduce, let us just say email phishing schemes by 10%, think of the amount of money that we could save to truly reinvest back into our partners in the industrial base that we need to stay on the competitive edge. And the only way that we saw fit to do this was to create this CMMC so we can ensure that we are doing everything we can do to buy down the risk of our adversaries stealing our hard work."

A close reading of the CMMC standard and public comments by the Office of the Under Secretary of Defense for Acquisition & Sustainment CMMC website provide valuable insight into the intent and implementation of the CMMC, including the specific maturity levels by which government contractors will be categorized. The five maturity levels (shown below) range from Basic Cyber Hygiene at Level 1 to Advanced/Progressive Cyber Hygiene at Level 5. Any company handling Controlled Unclassified Information (CUI) will be required at a minimum to meet the requirements of Level 3, Good Cyber Hygiene. It is anticipated that 30% of government contractors will be required to meet the Level 3 requirements, with less than 1% of contractors expected to be held to the requirements of either Level 4 or Level 5.

A Cybersecurity Model for Manufacturers & DOD Contractors in Five Levels



To be deemed compliant with Level 3, a government contractor must implement and maintain all 110 of the controls specified in the NIST 800-171 standard, along with 20 additional controls. Those 130 controls for Level 3, along with requirements for other levels, are listed in the CMMC model. While NIST 800-171 provides a foundation for Level 3 of CMMC, CMMC introduces multiple additional levels of cybersecurity into the DoD's evaluation of contractors. In addition to assessing the maturity of a company's implementation of cybersecurity controls, CMMC also will assess the company's institutionalization of cybersecurity practices and processes, as shown in the diagram.

Implications for Manufacturers and DoD Contractors

If you are doing work with the government, even if it is beyond the DoD's Defense Industrial Base (DIB), you should already plan for CMMC requirements because many anticipate it will likely quickly spread across other government agencies as an RFI and RFP requirement.

Implementation of CMMC is expected to impact a broad range of entities that do business with the DoD. Here is a look at seven areas in which those entities are likely to be affected by the new policy:

1. All government contractors working with the DoD will need to become CMMC-certified by passing an independent CMMC audit to verify they have met the appropriate level of cybersecurity for their business. The CMMC level required will be specified for each procurement in its solicitation.
2. The government contractor will be required to meet the appropriate certification level at the time of contract award.
3. Prime contractors must flow down the appropriate CMMC requirement to the subcontractors they intend to use for a specific contract. Verification of the status of the subcontractors' certifications will also be the responsibility of the Prime.
4. The DoD contracting officer will determine the appropriate CMMC level for the contracts they award and administer. Not all contracts require the highest level of security, and the level required for a particular contract will be specified in Sections L and M of the solicitation and the resulting contract.
5. During the CMMC Pilot Program, the inclusion of a CMMC requirement in any solicitation will require the approval of the OUSD for Acquisition and Sustainment.
6. The cost of preparing for a CMMC audit and becoming certified will be an "allowable cost" to government contracts. While DCAA has not issued specific guidance yet, it is the opinion of most experts in accounting and compliance that the cost will almost certainly be an indirect cost, probably G&A. Audits will be performed by an independent CMMC Third-Party Assessment Organization (C3PAO) that has been accredited by the CMMC Accreditation Body.
7. The CMMC Accreditation Body is an independent not-for-profit organization that is responsible for training and certifying independent C3PAO auditors.

Timeline of CMMC 2.0 Milestones

At the time, the government estimated it would take up to 24 months for CMMC 2.0 rulemaking finalization. And, because 1.0 had a phased approach targeting 2025 as a date for full requirements in RFPs and RFIs, many organizations have believed they have until 2025 to become compliant.

However, in May of this year, the DoD indicated the final rules could be complete by March 2023. As such, contractors may begin to see CMMC requirements in RFIs as early as May 2023.

And, unlike 1.0 where contractors did not need certification at bid, with 2.0 organizations will have to be certified at the appropriate contract level with package submissions. That means the timeframe to be CMMC compliant for many organizations is now much shorter than some may have thought.

If you are an organization wanting to bid on or renew contracts in early 2023, and you have not already begun your CMMC 2.0 journey, now is the time to get certified at the appropriate CMMC level you will need for those contracts.

So, it is important to think about the contracts you are going to want to go after. Will you have upwards of a year to get your certification complete before submitting your bid package?

Reasonable Timelines

No two organizations will have the same timelines and expenses related to CMMC 2.0 certification. There are a range of factors in play such as organization size and location. As such, organizations should expect variance in timelines and costs across the industry.

If your team members are still focused on the 2025 deadline, now is the time to shift away from that perspective.

First, the DFARS clauses already have control requirements. The 2025 date some stay focused on was for CMMC only. If you have DFARS obligations in your existing contracts, you will need to meet those now or be at risk of breach of contract.

So, if you have not already met those standards, what are you looking at in terms of a realistic CMMC 2.0 timeline?

The reality is, from start to finish, you might be looking at a process that could take a full year to traverse.

What would that look like? Here is an example:

Let us say you target getting started in May 2023 when it is anticipated to show up in RFPs. You will need to create your System Security Plan (SSP), which depending on the size of your organization could take about six months to complete and ensure accuracy. For smaller organizations, your SSP might be about 100 pages, but the larger you are, the larger your SSP will be, and it is not unrealistic to see some of those plans spanning 1,000 pages.

Once you have created your SSP, you will need to identify your Plan of Action and Milestones (POA&M) to demonstrate how you plan to close the gaps for standards you are not meeting now.

After that, if you are required to get an assessment from a Certified Third-Party Assessment Organization (C3PAO), you are going to need to select one and get on their calendar. Right now, there are about 21 C3PAOs listed in the marketplace. With the volume of organizations that will need assessments, do not be surprised if it takes a while to get that process started. And, even when that happens, it may take several months to complete that process.

From start to finish, if everything goes in your favor, your organization could anticipate this entire timeline to span about a year. If you are targeting May 2023 and have not started, you are already behind.

Budget Planning

Early government estimates for CMMC 1.0 Level 3 certification, which is now the same as CMMC 2.0 Level 2, were about $51,000. Contractors could then modify operating costs and overhead to absorb that amount and then build it back into the rate submitted to the government.

However, those numbers may be short of the real mark. Right now, published rates for a Level 2 assessment are already more than $60,000.

Reduce Breach of Contract Exposure

We can talk a lot about CMMC 2.0 as an effective way to reduce cyber risk, but in the end, what it is really about is ensuring you can reduce your exposure to breach of contract. If you do not meet government obligations for your DFARS and CMMC requirements, your organization may be subject to a breach of contract.

How do you ensure you do not go down that path? Here are 3 recommendations:

1. Ensure you have uploaded your SPRS score to the government database. Be honest and accurate. Remember, the government says you should not submit your SPRS unless you have completed your SSP. So, you will need to get through the SSP process before submitting your SPRS. River Run can help you simplify your SSP and POA&M processes.

   Point of caution: If you are a small or medium size contractor and you say your SPRS score, for example, is 110, there is a decent chance you are setting yourself up for an independent government audit. Officials have indicated they would

rather see a lower initial SPRS score that improves over time. That means they want to see what is accurate and what shows a rate of progression to meet total goals and objectives. If you have not done your SSP, do not upload your SPRS.

2. If you are self-attesting to CMMC 2.0 Level 1, be sure you fully understand what your organization is committing to. Even at Level 1, the business owner (CEO, COO, board, etc.) signing documents will be legally bound to document accuracy. The new Civil Fraud division can use this against you if you are willfully misrepresenting your cyber practices.
3. Even if a C3PAO certifies you at CMMC 2.0 Level 2, you will need to ensure resiliency to withstand an attack to prevent a claim against performance and schedule deficiencies. A C3PAO will only look at the goals and objectives defined by DoD under NIST 800-171. That is not a silver bullet, and it was never designed to be. Be sure your organization understands all of the obligations to which you may be exposed. Do you have data breach notification requirements in the states you operate in? If you meet the requirements that trigger a breach notification — and do not do so — those financial penalties alone could force you out of business or impact your organization in a way that you cannot perform at the same level of fidelity to the government.

Looking Forward

Should you anticipate a future CMMC 3.0? Likely. NIST has put out a call for comments on 800-171 revision 3, which is included in CMMC 2.0 requirements. CMMC was always meant to be dynamic and flexible for the cyber threat landscape. What might a CMMC 3.0 include? Maybe changes reflected in NIST 800-171 v3, and possibly also results from common findings of the C3PAO audits.

Assisting You with Your Organization's Compliance Needs

With manufacturers and government contractors facing a new regulatory reality in which they will be evaluated for CMMC compliance by an independent, sanctioned third-party auditor, River Run stands ready to support your efforts to comply with CMMC 2.0 and all future iterations.

River Run's R-Security portfolio and CIO Services support relevant technical requirements within the new model related to multi-factor authentication, identification and access controls, data encryption, and more. Our CIO and Technical Services teams have been diligent about keeping abreast of new DoD policies. We have taken the necessary steps to ensure that our processes and procedures are properly aligned with CMMC and NIST 800-171 standards.

For information on how River Run can support and simplify your company's compliance with federal government requirements, visit us at river-run.com or call us at (414) 228-7474 for a no obligation conversation with a member of our CIO Services Team.