SheppardMullin
Government Contracts & Investigations Blog
Latest updates on Developments Affecting Government Contracts & Investigations

DOD Updates Its Cybersecurity Certification Program – CMMC 2.0: What Contractors Need to Know

By Townsend Bourne & Nikole Snyder on November 10, 2021

POSTED IN CYBERSECURITY, DEPARTMENT OF DEFENSE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

On November 4, 2021, the Department of Defense ("DOD") **announced** several changes to the Cybersecurity Maturity Model Certification ("CMMC") program – the program that DOD intends to use to enhance the security of the defense industrial base through assessments and third-party cybersecurity certifications.**[1]** The new version of the program – "CMMC 2.0" – is a result of DOD's internal review of the CMMC program implemented thus far ("CMMC 1.0"), which began following the release of an **interim rule** in September 2020, and included review of over 850 public comments. DOD intends to engage in additional rulemaking to refine and finalize CMMC 2.0. Although the overall goal of the program remains focused on safeguarding sensitive unclassified information, CMMC 2.0 includes several important differences from the original program, as discussed in greater detail below.

Key Differences Between CMMC 1.0 and CMMC 2.0

DOD's announcement indicates it plans to update the CMMC program to streamline the model, reduce assessment costs, and provide for more flexible implementation. In particular, CMMC 2.0:

- Reduces the total number of assessment levels from 5 to 3;
- Allows for a self-assessment at Level 1 and at Level 2 (if the contractor is not handling "critical national security information");
- Aligns the required practices with cybersecurity standards issued by the National Institute of Standards and Technology (NIST);
- Reduces the total number of required security practices;
- Increases oversight of third-party assessors;
- Allows Plans of Action & Milestones (POA&Ms) and waivers to CMMC requirements under certain, limited circumstances; and
- Alters the timeline for compliance (to be required when the rulemaking is complete, estimated to be in 9-24 months).

For ease of comparison, the charts below identify the key features of CMMC 1.0 (prior version) as compared to CMMC 2.0 (new version):

CMMC 1.0		
Level	**Model/Practices**	**Assessment**
1 – Basic	17 practices	Third-party
2 – Intermediate	72 practices + 2 maturity processes	N/A
3 – Good	130 practices + 3 processes	Third-party
4 – Proactive	156 practices + 4 processes	N/A
5 – Advanced	171 practices + 5 processes	Third-party

CMMC 2.0		
Level	**Model/Practices**	**Assessment**
1 – Foundational	17 practices	Annual self-assessment
2 – Advanced	110 practices aligned with NIST SP 800-171	Triannual third-party assessments for critical national security information Annual self-assessment for select programs
3 – Expert	110+ practices based on NIST SP 800-172	Triannual government-led assessment

Notably, CMMC 2.0 aligns Level 2 with current DOD regulations regarding protecting Controlled Unclassified Information ("CUI") (*i.e.*, DFARS 252.204-7012; 252.204-7019;

252.204-7020). These regulations already mandate NIST SP 800-171 compliance as the minimum level of security for contractors handling CUI, while also including a requirement for self-assessment (or DOD assessment) against the NIST SP 800-171 controls and an associated report in the Supplier Performance Risk System.

Plans of Action and Milestones ("POA&Ms") and Waivers

In response to industry concerns that CMMC would mandate strict compliance without room for plans of action and milestones ("POA&Ms") to meet certain requirements, DOD intends under CMMC 2.0 to allow contractors with POA&Ms to receive contract awards, while still working to achieve compliance. DOD plans to identify a baseline number of requirements that must be achieved prior to such an award, but will allow the remaining requirements to be addressed in a POA&M with a clearly defined timeline.

Unlike the prior version, CMMC 2.0 also will include a limited waiver process to exclude CMMC requirements from "acquisitions for select mission critical requirements." Although details are not yet available, DOD announced these waivers will be temporary, and will require prior approval from senior DOD leadership. Additional information on the waiver process will be forthcoming during the rulemaking.

Implementation Timeline for CMMC 2.0

The changes outlined above are merely proposed at the present time – they will be implemented through the formal rulemaking process, which will include additional opportunities for public comment. DOD anticipates the rulemaking process will take anywhere from 9-24 months, and contractors will not be required to comply with CMMC 2.0 until the forthcoming rules go into effect.

This differs significantly from the prior timeline for CMMC 1.0. As discussed previously **here** and **here**, CMMC 1.0 included pilot programs and gradual implementation, culminating with the mandate for widespread inclusion of the CMMC requirements in all DOD solicitations by October 2025. For CMMC 2.0, there currently is no mention of pilot programs, and in fact, DOD is suspending the current CMMC pilot program while the rulemaking process is ongoing. However, it also appears the timeline for implementation has been accelerated, as DOD stated CMMC 2.0 will become a contract requirement once the rulemaking is complete

(in 9-24 months). Presumably, this means all contractors will need to prepare for CMMC compliance by November 2023, at the latest.

Putting it all into Practice

Although currently there is limited information available on DOD's CMMC 2.0, we expect more detailed information will be released as the rulemaking process continues to unfold. DOD has also announced it is exploring the idea of offering incentives to contractors who voluntarily obtain a CMMC certification while the rulemaking is ongoing, but no further information on that is yet available.

In the meantime, DOD contractors should be following closely all proposed cybersecurity developments and prepare for the implementation of CMMC 2.0 by continuing to monitor and enhance their cybersecurity posture.

FOOTNOTES

[1] DOD initially published an announcement (styled as an Advanced Notice of Proposed Rulemaking) in the Federal Register on November 5, 2021, but then quickly withdrew it. You can read a copy of the ANPR **here**, although it no longer is available in the Federal Register.

Government Contracts & Investigations Blog

Copyright © 2022, Sheppard, Mullin, Richter & Hampton LLP. All Rights Reserved.