DoD Cybersecurity Maturity Model Certification

CMMC 2.0 Explained

17 Dec 2021

#15 in the Blue Cyber Education Series
What happened?

- The DFARS Clause 252.204-7021, went into federal rule-making and the result was a revamp of the original plan.
  - The original plan of CMMC assessments and timelines to require DoD contractors pre-certified as to their cybersecurity capabilities was found to be needing revision.
- The new plan, being called CMMC 2.0, reverts the requirements to those already in place in every contract, the requirements of DFARS Clause 252.204-7012.
  - There might be requirements beyond DFARS Clause 252.204-7012, for some (few) contractors, but we won’t know until late 2022 at the earliest. The DCMA direction is to focus on DFARS 7012 compliance.
  - Listen to the best message on this subject from the DCMA Director here: https://www.preveil.com/resources/webinar-john-ellis-on-cmmc-2-0/
Why did the DoD make these changes?

- The Department values feedback from industry, Congress, and other stakeholders and received over 850 public comments in response to the interim rule establishing CMMC 1.0.

- These comments focused on the need to enhance CMMC by
  1. reducing costs, particularly for small businesses;
  2. increasing trust in the CMMC assessment ecosystem; and
  3. clarifying and aligning cybersecurity requirements to other federal requirements and commonly accepted standards.

- CMMC 2.0 was designed to meet these goals, which also contribute toward enhancing the cybersecurity of the defense industrial base.
The “Expert” level is currently under development, will be a subset of NIST SP 800-172 requirements.

The “Advanced” level will be equivalent to DFARS Clause 252.204-7012. Law since 2017

The “Foundational” level will be equivalent to the FAR Clause 252.204-21. Law since 2013

The rulemaking process and timelines can take 9-24 months.

CMMC 2.0 will become a contract requirement once rulemaking is completed. The publication of materials relating to CMMC 2.0 reflect the Department’s strategic intent with respect to the CMMC program; however, CMMC 2.0 will not be a contractual requirement until the Department completes rulemaking to implement the program.
DoD Depiction of Proposed Assessments

LATE 2022 AT THE EARLIEST

CMMC 2.0 tailors model and assessment requirements to the type of information being handled

**Model**

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
<th>Assessments</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEVEL 3</td>
<td>Expert, 110+ practices based on NIST SP 800-172</td>
<td>CUI, highest priority programs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Triennial Gov't-led</td>
</tr>
<tr>
<td>LEVEL 2</td>
<td>Advanced, 110 practices aligned with NIST SP 800-171</td>
<td>CUI, prioritized acquisitions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Triennial Third-Party</td>
</tr>
<tr>
<td>LEVEL 1</td>
<td>Foundational, 17 practices</td>
<td>CUI, non-prioritized acquisitions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Annual Self-Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FCI, not critical to national security</td>
</tr>
</tbody>
</table>

**Note:** The information in this presentation reflects the Department’s strategic intent with respect to the CMMC program. The Department will be engaging in rulemaking and internal resourcing as part of implementation, and program details are subject to change during these processes.
Proposed Overview of Assessments

LATE 2022 AT THE EARLIEST

CMMC 2.0 implements tiered assessment requirements based on the sensitivity of the information shared with a contractor.

Upon implementation of CMMC 2.0:

• Contractors who do not handle information deemed critical to national security (Level 1 and a subset of Level 2) will be required to perform annual self-assessments against clearly articulated cybersecurity standards.

• Contractors managing information critical to national security (a subset of Level 2) will be required to undergo third-party assessments.

• The highest priority, most critical defense programs (Level 3) will require government-led assessments.
Proposed Self-Assessments

LATE 2022 AT THE EARLIEST

The Department views Level 1 ("Foundational") as an opportunity to engage its contractors in developing and strengthening their approach to cybersecurity. Because Level 1 does not involve sensitive national security information, DoD intends for this Level to allow companies to assess their own cybersecurity and begin adopting practices that will thwart cyber-attacks.

Likewise, a subset of programs with Level 2 ("Advanced") requirements do not involve information critical to national security, and associated contractors will only be required to conduct self-assessments.

Contractors will be required to conduct self-assessment on an annual basis, accompanied by an annual affirmation from a senior company official that the company is meeting requirements. The Department intends to require companies to register self-assessments and affirmations in the Supplier Performance Risk System (SPRS).

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2021-4521, 22 Dec 2021
New Documentation Guides

https://www.acq.osd.mil/cmmc
Plan of Actions and Milestones (POA&Ms)  
**LATE 2022 AT THE EARLIEST**

With the implementation of CMMC 2.0, the Department intends to allow companies to receive contract awards with a Plan of Actions and Milestones (POA&M) in place to complete CMMC requirements.

The Department’s intent is to specify a baseline number of requirements that must be achieved prior to contract award, in order to allow a remaining subset to be addressed in a POA&M within a clearly defined timeline.

The Department also intends to specify a small subset of requirements that cannot be on a POA&M in support of achieving a CMMC certification.
So what has changed?

A re-focus on the FAR and DFARS requirements.

- **FAR Clause 252.204-21** still requires 15 security controls with no POAM. Law since 2013.
  
  This is the proposed Foundational Level of CMMC 2.0

- **DFARS Clause 252.204-7012** still requires 110 security controls implemented as the definition of adequate protection for DoD CUI. Law since 2017.
  
  This is the proposed Advanced Level of CMMC 2.0

- CMMC 2.0 will become a contract requirement once rulemaking is completed. Late 2022 at the earliest.
Resources

- DoD OSD A&S  CMMC 2.0 Webpage

- CMMC 2.0 FAQ (changing every week)

- How will my organization know what CMMC level is required for a contract?
  - Once CMMC 2.0 is implemented, DoD will specify the required CMMC level in the solicitation and in any Requests for Information (RFIs), if utilized.

- Will my organization need to be certified if it does not handle CUI?
  - DoD’s intent under CMMC 2.0 is that if a DIB company does not process, store, or transmit Controlled Unclassified Information (CUI) on its unclassified network, but does process, store or handle Federal Contract Information (FCI), then it must perform a CMMC Level 1 self-assessment and submit the results with an annual affirmation by a senior company official into SPRS.
Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.
- This presentation and other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage: https://www.safcn.af.mil/Organizations/CISO-Homepage/Small-Business-Cybersecurity-Information/
- Please provide questions, feedback or if you just want to talk about your cyber security/data protection questions to Kelley.Kiernan@us.af.mil
  
  ➢ Daily Office Hours for answering/researching your questions about DAF Small Business cybersecurity and data protection!

  ➢ Every Tuesday, dial in for the DAF CISO Small Business Cybersecurity Ask-Me-Anything. Register in advance for this Zoom Webinar: https://www.zoomgov.com/webinar/register/WN_CHsGAoWXTJSU5cDvEmQQHQ
The Blue Cyber Education Series for DoD Small Businesses on DAF CISO webpage


Every Tuesday Small Business Cybersecurity Ask-Me-Anything
Register in advance for this Zoom Webinar:
https://www.zoomgov.com/webinar/register/WN_CHsGAoWXTJSU5cDvEmQQHQ

Distribution Statement A: Approved for public release. Distribution is unlimited. Case Number: AFRL-2021-4521, 22 Dec 2021