Published on *The National Law Review* https://natlawreview.com

CMMC Level 3: Strict Scoping and Expansive Requirements

Article By:

Jessica McGahie Sawyer

Brian Long

James S. Mann

Elizabeth Hummel

Daniel P. Graham

David Sorenson

In this series of articles, we explore the different certification requirements of CMMC Levels 1, 2 and 3; the impact on contractors and external service providers; and proposed next steps. Read our initial summary here, our Level 1 summary here and our Level 2 summary here.

On December 26, 2023, the US Department of Defense (DoD) published its long-awaited proposed rule codifying the Cybersecurity Maturity Model Certification (CMMC) Program. Comments on the proposed CMMC rule were due February 26, 2024.

In addition to incorporating the largest number of individual security requirements, CMMC Level 3 applies some of the strictest scoping requirements, while lacking clarity in its standard of applicability. Additionally, Level 3 requires Federal contractors to obtain a perfect score on a Level 2 Certification Assessment by a CMMC Third-Party Assessment Organization (C3PAO) before the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DCMA DIBCAC) will conduct the Level 3 assessment. While the uncertainty of applicability and the strict scoping requirements appear burdensome, the narrow subset of contractors to whom Level 3 will apply and the likelihood that these contractors have been tracking CMMC developments may mitigate any burdens. Those contractors required to certify as Level 3 will likely already have a history of compliance with Defense Federal Acquisition Regulation Supplement (DFARS) requirements and experience with government-led assessments.

Commenters on the proposed CMMC rule seem to believe that the DoD will not be able to

consistently identify critical information, which would lead to unpredictable application of Level 3. Given the significant financial burden created by Level 3 implementation, the DoD may wish to address this uncertainty.

In Depth

APPLICABILITY

Practically speaking, because the DCMA DIBCAC will perform CMMC Level 3 assessments itself, rather than a third party as with CMMC Level 2 Certification Assessments, it is likely that only contractors required to have a Level 3 assessment for their contract performance will be able to obtain one. This likely means that contractors cannot obtain their certification in advance of their contract, which may be troublesome for contractors that fail their assessment.

Level 3 does not have a clear-cut scope of applicability, unlike Level 1, which is applicable to contractors that handle Federal Contracting Information, and Level 2, which is applicable to contractors that handle Controlled Unclassified Information (CUI). Under the proposed CMMC rule, Level 3 is applicable to contractors that handle particularly sensitive CUI. As a result, CUI requires defense against sophisticated threat actors, or Advanced Persistent Threats (APTs). The proposed CMMC rule does not specify which CUI is considered "particularly sensitive," providing little insight for contractors to determine whether they would be subject to Level 3. Since this is a subjective standard, it is not clear that Level 3 applicability will be evenly applied across all contractors. Level 3 will most likely be required for the programs and contracts already subject to the National Institute of Standards and Technology's (NIST) *Enhanced Security Requirements for Protecting Controlled Unclassified Information* (SP 800-172), as the source of the Level 3 controls. NIST SP 800-172 is intended to apply to programs and contracts processing CUI associated with "a critical program or a high value asset."

However, most contractors will not need to worry about the additional requirements for Level 3. DoD estimated that Level 3 would only apply to a small subset of government contractors: roughly 1% (CMMC Proposed Rule Preamble, Table 3 – Estimated Number of Entities by Type and Level). The CMMC requirements will not be imposed until DoD updates the related implementing rule, DFARS 252.204-7021. Perhaps more information about when Level 3 will be available will be revealed in the coming months, possibly when updates or replacements to DFARS 252.204-7021 are made to require specific CMMC certification levels in future contracts.

SCOPE

The CMMC Assessment Scope for Level 3 includes the following assets as in scope: CUI Assets, Security Protection Assets and Specialized Assets. For a more in-depth look at the definitions of these assets, please consult our article on CMMC Level 2. These assets are assessed against all CMMC security requirements. Contractors may, however, use intermediary devices (devices that serve as a bridge between a contractor's operational technology and network) to provide the capability for a Specialized Asset to meet one or more CMMC security requirements. In addition, the Level 2 Certification Assessment must occur prior to the Level 3 assessment and must include the

same scope as the Level 3 assessment. This means that a Level 2 Certification Assessment in preparation for Level 3 may have a larger scope than a standard Level 2 Certification Assessment. For example, Specialized Assets undergo a review of the system security plan (SSP) only in a Level 2 Certification Assessment but are assessed against all CMMC security requirements in a Level 3 assessment. When obtaining the precursor Level 2 assessment, those Specialized Assets must be fully assessed during the Level 2 Certification Assessment.

Assets that cannot process, store or transmit CUI and that do not provide security protection for CUI assets are considered out of scope. Contractors should prepare to justify the inability of an Out-of-Scope Asset. For a table of asset categories and their associated descriptions and requirements, see 32 C.F.R. § 170.19(d)(1), Table 2.

REQUIREMENTS

In order to undergo a Level 3 assessment, a contractor must first achieve a Level 2 Final Certification Assessment on systems in the Level 3 assessment scope. A Level 2 Final Certification can only be achieved with a perfect score for the Level 2 assessment by a C3PAO (*i.e.*, an assessment that has closed any open plan of action and milestones (POA&M) items and is not a self-assessment). All Level 2 requirements must result in a finding of MET prior to the Level 3 assessment (more on assessment findings and the MET requirement below).

See the table below for an in-depth description of the Level 3 security requirements (32 C.F.R. § 170.14 (c)(4), Table 1).

Security Requirement No.	CMMC Level 3 requirements (Selected NIST SP 800-172 Requirement with DoD ODPs italicized)
AC.L3-3.1.2e	Restrict access to systems and system components to only those information resources that are owned, provisioned or issued by the organization.
AC.L3–3.1.3e	Employ *secure information transfer solutions* to control information flows between security domains on connected systems.
AT.L3–3.2.1e	Provide awareness training *upon initial hire, following a significant cyber event, and at least annually*, focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches and suspicious behaviors; update the training *at least annually* or when there are significant changes to the threat.
AT.L3–3.2.2e	Include practical exercises in awareness training for *all users, tailored by roles, to include general users, users with specialized roles, and privileged users*, that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.
CM.L3–3.4.1e	Establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components.

CM.L3–3.4.2e	Employ automated mechanisms to detect misconfigured or unauthorized system components; after detection, *remove the components or place the components in a quarantine or remediation network* to facilitate patching, re-configuration or other mitigations.
CM.L3–3.4.3e	Employ automated discovery and management tools to maintain an up-to-date, complete, accurate and readily available inventory of system components.
IA.L3–3.5.1e	Identify and authenticate *systems and system components, where possible*, before establishing a network connection using bidirectional authentication that is cryptographically based and replay resistant.
IA.L3–3.5.3e	Employ automated or manual/procedural mechanisms to prohibit system components from connecting to organizational systems unless the components are known, authenticated, in a properly configured state or in a trust profile.
IR.L3–3.6.1e	Establish and maintain a security operations center capability that operates *24/7, with allowance for remote/on-call staff*.
IR.L3–3.6.2e	Establish and maintain a cyber-incident response team that can be deployed by the organization within *24 hours*.
PS.L3–3.9.2e	Ensure that organizational systems are protected if adverse information develops or is obtained about individuals with access to CUI.
RA.L3–3.11.1e	Employ *threat intelligence, at a minimum from open or commercial sources, and any DoD-provided sources*, as part of a risk assessment to guide and inform the development of organizational systems, security architectures, selection of security solutions, monitoring, threat hunting, and response and recovery activities.
RA.L3–3.11.2e	Conduct cyber threat hunting activities *on an on-going aperiodic basis or when indications warrant*, to search for indicators of compromise in *organizational systems* and detect, track and disrupt threats that evade existing controls.
RA.L3–3.11.3e	Employ advanced automation and analytics capabilities in support of analysts to predict and identify risks to organizations, systems and system components.
RA.L3–3.11.4e	Document or reference in the system security plan the security solution selected, the rationale for the security solution, and the risk determination.
RA.L3–3.11.5e	Assess the effectiveness of security solutions *at least annually, or upon receipt of relevant cyber*

	threat information, or in response to a relevant cyber incident, to address anticipated risk to organizational systems and the organization based on current and accumulated threat intelligence.
RA.L3–3.11.6e	Assess, respond to and monitor supply chain risks associated with organizational systems and system components.
RA.L3–3.11.7e	Develop a plan for managing supply chain risks associated with organizational systems and system components; update the plan *at least annually, and upon receipt of relevant cyber threat information, or in response to a relevant cyber incident*.
CA.L3–3.12.1e	Conduct penetration testing *at least annually or when significant security changes are made to the system*, leveraging automated scanning tools and ad hoc tests using subject matter experts.
SC.L3–3.13.4e	Employ *physical isolation techniques or logical isolation techniques or both* in organizational systems and system components.
SI.L3–3.14.1e	Verify the integrity of *security critical and essential software* using root of trust mechanisms or cryptographic signatures.
SI.L3–3.14.3e	Ensure that *Specialized Assets including IoT, IIoT, OT, GFE, Restricted Information Systems and test equipment* are included in the scope of the specified enhanced security requirements or are segregated in purpose-specific networks.
SI.L3–3.14.6e	Use threat indicator information and effective mitigations obtained from, *at a minimum, open or commercial sources, and any DoD-provided sources*, to guide and inform intrusion detection and threat hunting.

ORGANIZATION-DEFINED PARAMETERS

The proposed rule revises the concept of organization-defined parameters (ODPs). Under NIST's *Assessing Enhanced Security Requirements for Controlled Unclassified Information* (SP 800-172A), each organization defines its own ODPs to allow for flexibility in assessing the controls of an organization based on its needs. However, for CMMC Level 3, the DoD has defined these ODPs to ensure a level of security commensurate with its expectations for contractors seeking Level 3 certification.

Levels 1 and 2 do not use ODPs. Since Level 2 codifies NIST SP 171 Rev. 2, the ODPs introduced by NIST SP 171 Rev. 3 will not be used by contractors for Levels 1 or 2. However, if the DoD revises the rule to take into consideration updates to NIST SP 171, ODPs may come into play for Levels 1 and 2. Draft Rev. 3 of NIST SP 800-171 adds ODPs and, as we discussed in our CMMC Level 2 article, this may introduce some tension when NIST SP 171 Rev. 3 becomes the current version of NIST SP 800-171 because DFARS 252.204-7012 follows the current release version of NIST SP

800-171, while CMMC specifically codifies Rev. 2 for Level 2, which may require contractors to satisfy the requirements of both Rev. 2 and Rev. 3 at the same time.

ASSESSMENT

To achieve a CMMC Level 3 Certification Assessment, all Level 3 security requirements must be MET or have a POA&M in place. Level 3 Certification Assessments are performed by the DCMA DIBCAC, which issues the Level 3 Certification Assessment certificates and uploads Level 3 Certification Assessment results into the CMMC instantiation of eMass (32 C.F.R. § 170.7(5)). Level 3 uses the CMMC scoring methodology: each control has a finding of MET, NOT MET or NOT APPLICABLE. However, unlike Level 2, the Level 3 assessment does not assign different scores to different controls; each control is only worth one point when MET. The Level 3 scoring methodology accounts for all Level 2 security requirements already being MET as a requirement for a Level 3 assessment, so points are only assigned for requirements unique to Level 3.

Contractors may implement a POA&M in the place of a security requirement only if the contractor has a finding of MET for 80% or more of Level 3 security requirements. Because only 24 controls were selected from NIST SP 800-172 as Level 3 controls, a contractor must have at least 20 controls pass the assessment (*i.e.*, the POA&M can only have up to four controls on it). In addition, the contractor will fail if the following controls are not passed (*i.e.*, if they are placed on the POA&M):

- IR.L3–3.6.1e Security Operations Center
- IR.L3–3.6.2e Cyber Incident Response Team
- RA.L3–3.11.1e Threat-Informed Risk Assessment
- RA.L3–3.11.6e Supply Chain Risk Response
- RA.L3–3.11.7e Supply Chain Risk Plan
- RA.L3–3.11.4e Security Solution Rationale
- SI.L3–3.14.3e Specialized Asset Security

If a contractor uses a POA&M and achieves the minimum score necessary to be certified, the contractor has a Conditional Certification Assessment; if the contractor meets the minimum score and has no POA&M, then it has a Final Certification Assessment. Where a POA&M is used, it must be closed out within 180 days of the initial assessment by arranging for the DMCA DIBCAC to perform a closeout inspection.

During the assessment, the DCMA DIBCAC may perform checks to ensure that all Level 2 security requirements are MET for in-scope assets. If the DCMA DIBCAC determines that a Level 2 security requirement is NOT MET, the assessment may be placed on hold or terminated (32 C.F.R § 170.18(c)(ii)).

REQUIRED AFFIRMATIONS

Like CMMC Levels 1 and 2, CMMC Level 3 introduces a requirement for affirmations that must be provided by a contractor’s senior official who is responsible for ensuring the contractor’s compliance with the CMMC Program.

These affirmations present a heightened risk to Federal contractors of False Claims Act violations (31 U.S.C. §§ 3729-3733). The annual affirmation, in particular, requires Federal contractors to be vigilant in maintaining their assessed environments, to identify and surface any changes that would affect the environment’s compliance with CMMC requirements and to have a process to ensure that

the senior officials making the affirmations have accurate and complete information regarding the entity's CMMC compliance.

EXTERNAL SERVICE PROVIDERS

Like CMMC Level 2, an External Service Provider (ESP) must be certified to the level of the contractor utilizing it. For Level 3, this means a contractor must only use an ESP that has a Level 3 Final Certification Assessment (32 C.F.R. § 170.19(c)(2)).

KEY TAKEAWAYS

- ODPs are no longer defined by each organization, but instead by DoD.
- ESPs that exist outside of the Federal contracting ecosystem and have clients who seek to become CMMC Level 3 certified may have a substantial amount of work ahead of them, including getting on the DCMA DIBCAC's schedule for CMMC Level 3 assessments.
- Uncertainty surrounding the type of data that requires a CMMC Level 3 certification may make it difficult for contractors processing CUI to predict the level of security they need to implement.

Since a government entity is performing the assessment, the Level 3 certification process may not be as quick as it is for Levels 1 or 2.

National Law Review, Volume XIV, Number 292

Source URL:https://natlawreview.com/article/cmmc-level-3-strict-scoping-and-expansive-requirements