KRATOS
READY FOR WHAT'S NEXT™

DECEMBER 2021

CMMC 2.0

Part 1-Framework Evolution

On 4 November 2021, the Department of Defense (DoD) released plans for CMMC 2.0, which significantly changes the existing CMMC compliance framework. CMMC 2.0 aims to streamline the certification process, reduce costs, and improve flexibility.

"The DoD ... delivered on what the internal review set out to accomplish: clarifying the standard, reducing the cost burden, improving scalability, and instilling greater trust and confidence in the CMMC ecosystem."

MATTHEW TRAVIS, CMMC-AB CEO

COST REDUCTION

Reduces costs by bringing back self-attestations on a limited basis

FLEXIBILITY

Acknowledges the evolving nature of security by allowing limited use of POAMs and exceptions

STREAMLINED PROCESS

Reduces compliance levels from 5 to 3 and removes ambiguous/subjective maturity requirements

"These updates will support businesses in adopting the practices they need to thwart cyber threats while minimizing barriers to compliance with DoD requirements."

JESSE SALAZAR, DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR INDUSTRIAL POLICY

EXECUTIVE SUMMARY

To better secure the Defense Industrial Base (DIB) supply chain without burdening companies with expensive and time-consuming certifications, the DoD revised the original CMMC framework and released CMMC 2.0 in November 2021. The revised framework will safeguard sensitive information and meet evolving threats while enhancing public trust in the DoD. CMMC 2.0 streamlines the level of effort necessary to meet compliance standards and minimizes the monetary cost of compliance for small and medium businesses. CMMC 2.0 reduces the number of compliance levels and reinstitutes (in limited capacities) Plans of Action and Milestones (POA&Ms) and self-attestations. This overhaul was implemented to help not only large companies become compliant, but also to encourage smaller DIB members to begin improving their cybersecurity posture.

Members of the Kratos CMMC Team, Cole French and Alexandra Santulli, have performed a deep dive on the CMMC 2.0 changes, held meetings with the CMMC-AB, and have worked closely with other industry partners to ensure that accurate information is being communicated about CMMC 2.0. This paper will address the major changes to the CMMC 1.0 framework.

Table of Contents

CMMC 2.0 Major Changes

After the initial CMMC 1.0 framework and Interim Rule were released in 2020, the CMMC-AB began collecting industry feedback via DoD working groups and steering groups. The feedback ultimately resulted in a revised framework, CMMC 2.0, that will be accompanied by supplementary rulemaking still to come. CMMC 2.0 is composed of 3 levels, which is a reduction from the 5 levels of certification present in CMMC 1.0. CMMC 1.0's Levels 2 and 4 have been eliminated. Although the complex nature of CMMC 1.0 and the continuously evolving nature of CMMC has caused frustration in the DIB, the DoD considers CMMC 2.0 a positive step forward. The points below are a snapshot of what's new. The subsequent sections of this paper will go into more detail, but below are the key points:

- Level 1 requires a self-assessment only.
- POA&Ms, previously prohibited in CMMC 1.0, will be allowed on a limited basis.
- Waivers (or exceptions) will be allowed on a limited basis.
- Maturity processes will no longer be included.
- All CMMC unique practices (Delta practices) will be removed.
- Organizations handling CUI will be required to obtain at least Level 2 certification.
- The nature of a Level 2 certification will be based on different types of CUI. These definitions are in development. The end result will be a small number of self-attestation Level 2 assessments.
- A Level 2 certification is a prerequisite to pursuing a level 3 certification.

What's the Same?

Not everything has changed, and much of the progress C3PAOs and DIB members have taken will still apply and ease CMMC certification.

- CMMC 2.0 still addresses FCI and CUI security concerns and divides levels based on what type of information an organization handles.
- Registered Practitioner (RP) and Provisional Assessor (PA) certifications are still valid and those individuals are still able to assist companies for CMMC 2.0 preparation.
- Certified C3PAOs are still able to assess or offer advisory services.
- Supplier Performance Risk System (SPRS) and Enterprise Mission Assurance Support Service (eMASS) are still the plan for submitting self-assessment and third-party assessment information, respectively.
- CMMC 2.0 does not alter the Level 1 controls. The difference is that CMMC 2.0 only requires a self-attestation for Level 1 certification.

Level Summary

Level 1 Foundational

The number of controls in CMMC 2.0 level 1 remains the same as in version 1.0 and applies only to companies handling FCI. Level 1 protects organizations handling information that requires protection but is not critical to national security.

There are 17 controls across 6 control families in the 2.0 level 1.

1. Access Control (AC)
2. Identification & Authentication (IA)
3. Media Protection (MP)
4. Physical Protection (PE)
5. System and Communications Protection (SC)
6. System and Information Integrity (SI)

The major difference for level 1 is the verification process. CMMC 2.0 only requires a self-assessment for level 1, as compared to CMMC 1.0, which required a C3PAO assessment. Level 1 self-attestation results must be uploaded in SPRS and be accepted by the DoD before official certification is granted.

Level 2 Advanced

CMMC 1.0 Level 2 contained 72 controls and 2 documented maturity processes. CMMC 2.0 removes the maturity processes across all levels. Additionally, the new level 2 absorbs the previous CMMC 1.0 level 3 controls. Subsequently, the CMMC 2.0 level 2 increases to 110 controls derived from NIST SP 800-171. Although CMMC 2.0 level 2 contains more controls than it's predecessor, it only spans 14 control families versus the previous level 2 which spanned 17 control families.

For organizations handling prioritized CUI acquisitions, level 2 compliance will be verified through a tri-annual C3PAO assessment with the results entered into eMASS. The DoD projects the majority of organizations seeking a level 2 certification will require a C3PAO assessment. However, in a select few instances, an organization will be able to self-assess for a level 2 certification. These instances are most likely reserved for organizations handling non-prioritized CUI acquisitions. The exact nature of non-prioritized acquisitions has yet to be determined.

Level 3 Expert

CMMC 2.0 level 3 incorporates the previous CMMC 1.0 level 4 and 5 controls. The exact number of controls for the CMMC 2.0 level 3 has not been finalized. Unlike CMMC 1.0, in order to attempt a level 3 certification, an organization must successfully achieve a level 2 certification. Once level 2 certified, an organization can apply for a level 3 delta assessment.

Level 3 assessments can only be conducted by government auditors. CMMC 2.0 level 3 is expected to include the 110 level 2 controls and select controls taken from NIST SP 800-172. Notably, a level 3 assessment will only cover the delta controls (i.e., those not in level 2). While NIST SP 800-171 helps protect all CUI handled by DoD contractors, NIST SP 800-172 (previously NIST SP 800-171B) focuses on protecting against Advanced Persistent Threats (APTs). It is unlikely that all DIB members will need a level 3 certification even if they handle CUI. The new framework and subsequent contracts will take into account the type of CUI handled before requiring a level 3 certification.

POA&Ms and Waivers

Many DIB members found the all or nothing approach of CMMC 1.0 daunting. Version 2.0 will allow POA&Ms but on a limited, approval-required basis and with strict time limits for implementation. The DoD and CMMC-AB estimate that the time limit for POA&Ms to be completed will be set at 180 days. The 180 day countdown period will begin upon contract award. After the fixed-time period has elapsed, a C3PAO will need to re-assess to validate closure of POA&Ms. Not all controls will be eligible for a POA&M. The DoD plans to release a priority list of controls that must be fully implemented in order to begin the formal assessment process. Any control on the priority list will be ineligible for a POA&M.

Waivers, for control exceptions, like POA&Ms, will be on a limited basis in select mission-critical instances. Exceptions will be timebound and the exact length of the exception will be determined on a case-by-case basis at time of contract. All exceptions will require DoD approval.

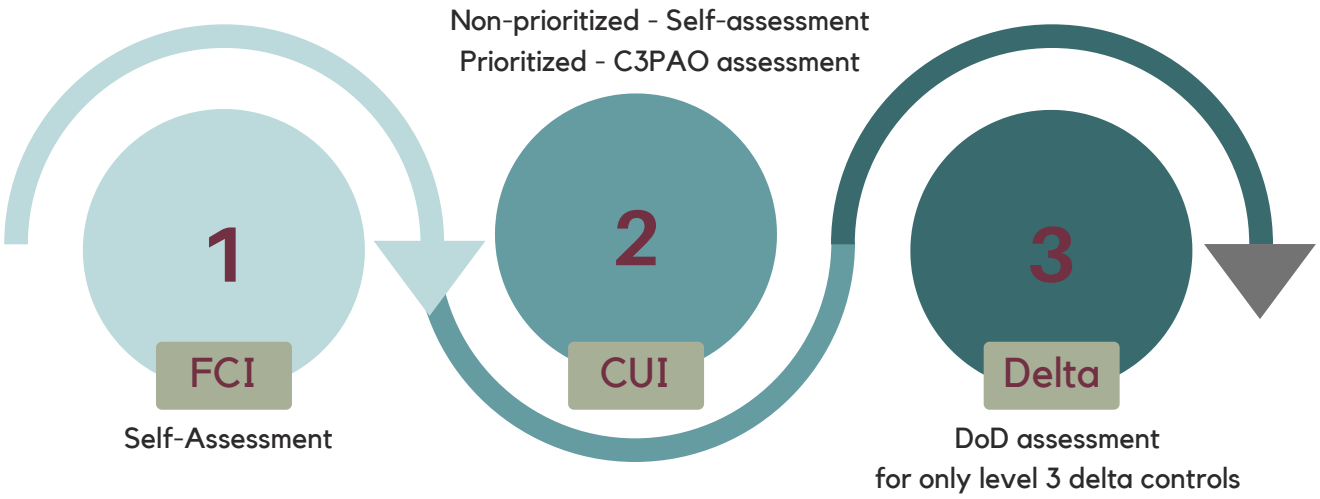
Reciprocity

Much like CMMC 1.0, many DIB members have posed questions regarding reciprocity. Both the CMMC-AB and DoD continue to imply that a reciprocity model will be released in the future; however, the exact nature of that reciprocity process is to be determined.

Choosing the Right Level for Your Organization

If your organization started the CMMC compliance process, there may be confusion on what level to pursue to continue going forward. Despite all the changes, the basic concepts remain largely the same. If your organization handles only FCI, level 1 is satisfactory. However, if your organization anticipates handling CUI in the near future or plans on competing for contracts with CUI, targeting a level 2 certification would be the next step. In either case, a level 1 self-assessment is a good stepping stone, especially for small DIB organizations. If your organization presently handles CUI, either basic or specified, pursuing a level 2 certification is the best path. The 110 controls in level 2 will put your organization in a good position should a level 3 certification become necessary.

Getting a head start on level two is prudent especially if your organization handles a category of specified CUI. The exact details are not available for determining the necessity of a level 3 certification, but it is likely companies handling specified CUI will be required to achieve a level 3 certification.



Key Takeaways

- CMMC 2.0 has 3 levels; however, the majority of contracts involving CUI will likely only require a level 2 certification, with a select few contracts requiring a level 3 delta assessment.
- Level 1 only requires a self-attestation and is designed to help smaller DIB organizations begin their security hardening process.
- DoD advises organizations to continue the CMMC implementation process using the NIST 800-171 controls.
- C3PAOs, Registered Practitioner (RP), and Provisional Assessor (PA) certifications are still valid credentials.

Anticipated CMMC 2.0 Clarification

According to the CMMC-AB and in cooperation with the DoD:

- The CMMC 2.0 Assessors Guide is expected to be released by the end of 2021.
- The scoping guide and reciprocity process are still in the developmental phase.
- The final rulemaking publication and cost estimates are expected in 2022.

Other helpful resources include Kratos' Advisory Services whitepaper and our CMMC 2.0 Factsheet. Plus, be sure and stay tuned for Part II of this whitepaper, where we'll discuss control changes, terminology updates, scoping and reciprocity guidance, POA&M specifics, and other details, as relevant. Finally, while all of these proposed changes are evaluated, Kratos will keep you abreast of the changes and provide you with valid guidance on how to best prepare for CMMC assessments when they begin.

About Kratos

Within the cybersecurity/warfare space, Kratos serves as a trusted advisor, supporting commercial companies and agencies through a full life cycle of system design, control implementation, and risk management processes. Most recently, Kratos was one of the first companies to be authorized as a CMMC Certified Third-Party Assessment Organization (C3PAO). Additionally, Kratos has years of robust compliance and certification experience with government and commercial standards and compliance frameworks requirements. In addition to being a C3PAO, Kratos was one of the first and largest Federal Risk and Authorization Management Program (FedRAMP) Third Party Assessment Organizations (3PAO). Kratos' compliance experience also includes the Payment Card Industry (PCI), Federal Information Security Management Act (FISMA) and the National Institute of Standards & Technology (NIST)/Risk Management Framework (RMF). Kratos is viewed as a trusted compliance and governance partner by the DoD, Federal Civilian Agencies, Intelligence Community (IC), and commercial organizations.

As an authorized C3PAO, Kratos is prepared to offer Advisory or Assessment services. Assessment services include scoping analyses, readiness assessments, penetration testing, and continuous monitoring. Advisory services include gap assessments, documentation, and process and engineering consulting services.

Kratos Defense & Security Solutions, Inc. (NASDAQ:KTOS) develops and fields transformative, affordable technology, platforms and systems for United States National Security affiliated customers, allies and commercial enterprises. Kratos is changing the way breakthrough technologies for these industries are rapidly brought to market through proven commercial and venture capital backed approaches, including proactive research and streamlined development processes. At Kratos, affordability is a technology, and we specialize in unmanned systems, satellite communications, cyber security/warfare, microwave electronics, missile defense, hypersonic systems, training, combat systems and next generation turbojet and turbo fan engine development.

For more information go to www.kratosdefense.com/cyber.