CYTELLIX

UPDATES TO CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

The Clock is Ticking for CMMC 2.0

cytellix.com
info@cytellix.com
(949) 215-8889

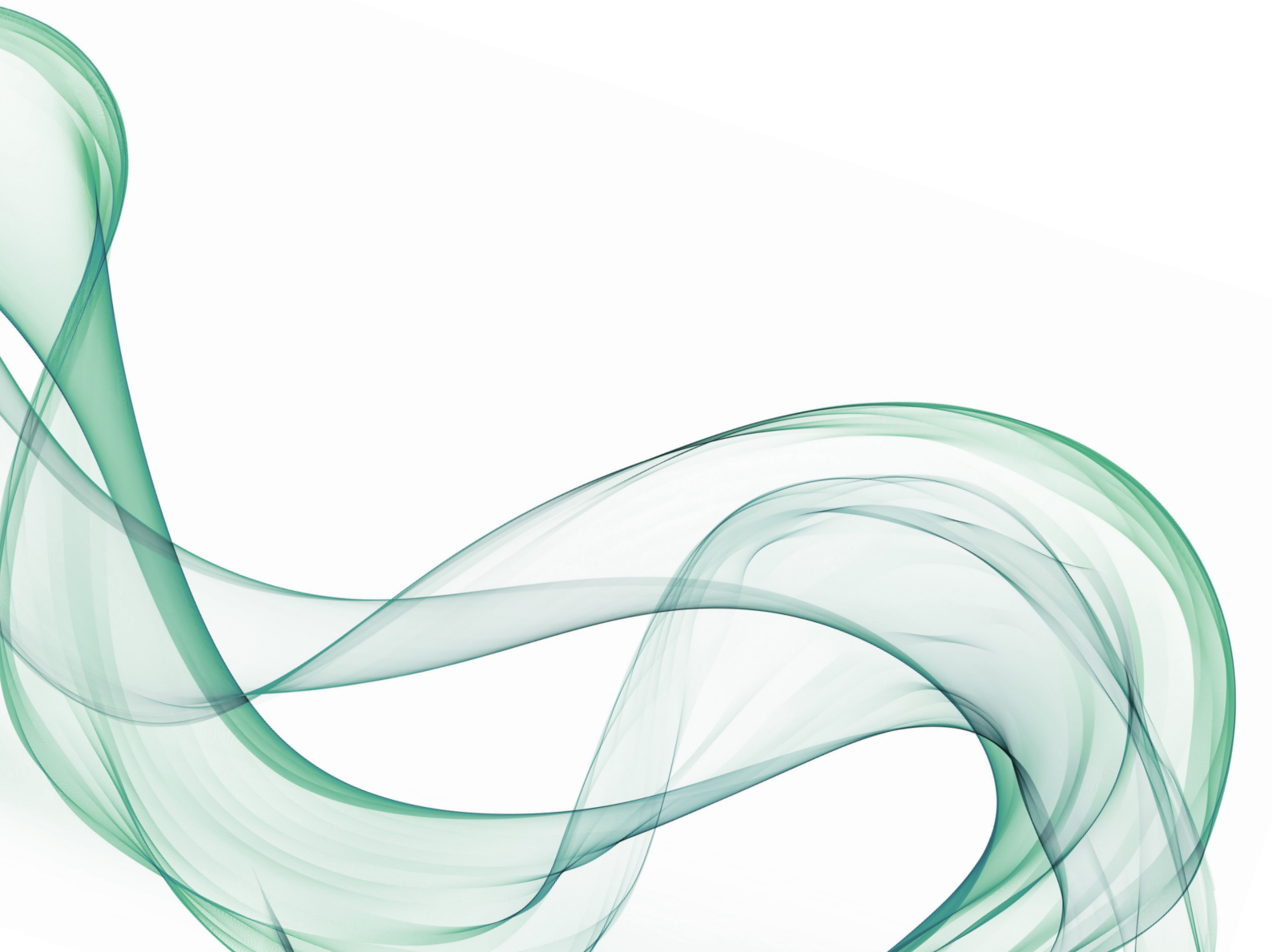
INTRODUCTION

This white paper provides an in-depth analysis of the Cybersecurity Maturity Model Certification (CMMC), with a particular focus on its latest iteration, CMMC 2.0. We outline the historical efforts leading to the current framework and present developments of the upcoming version, aligning with a 5-year projected plan.

The Department of Defense (DoD) introduced the Cybersecurity Maturity Model Certification (CMMC) framework in September 2020 to bolster cybersecurity within the Defense Industrial Base (DIB). This paper aims to offer a comprehensive look at the journey of CMMC up to this point and the direction it is headed with CMMC 2.0.

The CMMC initiative began as an effort to standardize cybersecurity measures across the DIB. It was designed to assess and enhance the cybersecurity posture of contractors working with the DoD. Over the past years, it has undergone various updates to address evolving security threats.

The DIB is a crucial component of national security, as it consists of contractors and suppliers responsible for developing, producing, and maintaining military and defense capabilities.



Here are some key reasons why the DoD introduced CMMC:

Standardizing Cybersecurity Measures

Before CMMC, there were disparate cybersecurity standards and practices across the DIB. CMMC aims to bring standardization and uniformity to how contractors and subcontractors manage sensitive information, thereby reducing the risk of cybersecurity incidents.

Protecting Controlled Unclassified Information (CUI)

The CMMC framework places a strong emphasis on safeguarding Controlled Unclassified Information, a category of sensitive data that, while not classified, still requires strict protection. The mishandling of CUI can pose significant risks to national security.

Vendor Accountability

CMMC provides a mechanism for the DoD to assess the cybersecurity maturity of its contractors and subcontractors. With the certification, contractors cannot just say they are secure; they must demonstrate their security measures through third-party assessments, increasing accountability.

Closing Security Gaps

The initiative aims to identify and close security gaps that might be exploited by adversaries. Cybersecurity threats are ever evolving, and the CMMC framework is designed to be adaptive to new risks and vulnerabilities, thereby providing more robust protection.

Building a Competitive Advantage for Compliant Businesses

CMMC not only levels the playing field but also gives compliant companies a competitive edge. Contractors who take cybersecurity seriously and meet the CMMC requirements are more likely to win DoD contracts.

Encouraging Proactive Cybersecurity Culture

The introduction of CMMC encourages a shift from a reactive to a proactive cybersecurity stance. Businesses in the DIB are now more incentivized to continuously improve their cybersecurity measures, not just meet the minimum requirements.

The Department of Defense (DoD) has officially submitted the CMMC 2.0 rule to the Office of Information and Regulatory Affairs (OIRA) for review. The review process is expected to be published in late October 2023. The CMMC rule should be finalized and included in government contracts by as early as Q1 2025.

Evolution from CMMC 1.0 to 2.0

CMMC 1.0 Overview

- **Level 1:** Comprised of 17 basic cybersecurity requirements based on NIST SP 800-171.
- **Level 2:** Included 72 practices, which extended the 65 NIST SP 800-171 requirements with an additional 7 practices.
- **Level 3:** Consisted of 130 practices, merging 110 from NIST SP 800-171 with 20 unique ones.
- **Level 4 & 5:** Added even more practices for more advanced cybersecurity needs.

CMMC 2.0 Overview

- **Level 1:** Maintains the 17 original practices, now requiring an annual self-assessment.
- **Level 2:** Streamlined to 110 practices based on NIST SP 800-171, focusing on critical national security information.
- **Level 3:** Features 110+ practices, introducing standards from NIST SP 800-172.

Key information on the Transition

The foundational cybersecurity requirements from NIST SP 800-171 remain constant. If your company is involved with Controlled Unclassified Information (CUI), the transition to CMMC 2.0 should have minimal impact on your existing practices.

Given the 12-18 month timeframe for companies, to prepare and achieve CMMC certification, it's crucial for the DIB to start planning and implementing CMMC 2.0 as soon as possible or they will likely find their contracts in jeopardy come 2025.

CMMC IN A NUTSHELL

What is the CMMC?

The CMMC defines a series of activities, procedures, compliance requirements, and certification expectations using an assessment framework that finds its genesis in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. The assessment framework outlines cybersecurity controls and processes required to protect the DIB and supply chain operating environment.

CMMC stands for "Cybersecurity Maturity Model Certification." The CMMC will encompass multiple maturity levels that range from "Basic Cybersecurity Hygiene" to "Advanced." The intent is to identify the required CMMC level in RFP sections L and M to us as a "go / no go decision."

Who are the Players?

Cyber-AB (Advisory Board)

The Cyber-AB is the official accreditation body of the Cybersecurity Maturity Model Certification (CMMC) Ecosystem and the sole authorized non-governmental partner of the U.S. Department of Defense in implementing and overseeing the CMMC conformance regime.

RPO

A Registered Provider Organization (RPO) is an organization that has been authorized by the CMMC Accreditation Body to provide pre-assessment consulting services to companies in the Defense Industrial Base (DIB) aiming to achieve CMMC certification. These organizations do not conduct the certification assessments themselves; rather, they help prepare companies for the assessment process.

RPOs are trained in the CMMC methodology and can offer insights and guidance on how to improve a company's cybersecurity posture to meet the required maturity level for certification. They can assist with tasks such as gap analysis, readiness assessments, and the development of necessary documentation.

It is particularly valuable for small to medium-sized companies in the DIB to engage with an RPO if they lack the in-house resources or expertise to navigate the complexities of the CMMC certification process. Utilizing the services of an RPO can help these companies better understand the certification requirements, identify areas for improvement, and work more efficiently towards achieving their desired certification level within the CMMC framework.

CMMC Third Party Assessment Organization (C3PAO)

The certification level for each organization needed to be validated by a CMMC Third Party Assessment Organization (C3PAO) that will be authorized and trained to do the work by an Accreditation Body. The CMMC approval will be tied to the C3PAO and available for the DoD to view when considering responses to a solicitation.

As defined by the Cyber-AB, a C3PAO, is an organization that is certified to perform an assessment of an organization seeking to become certified as complaint at a specific level. C3PAO's do not provide preparation or consulting services prior to the certification assessment nor can a CMMC Certified Assessor (CCA) who works for a C3PAO provide pre-assessment services and then assess. Prepare an approach that will provide your organization with the proper preparation in advance of the final assessment process.

"The DoD will only accept CMMC assessments provided by the Government or an authorized and accredited C3PAO or certified CMMC Assessor. C3PAOs shall use only certified CMMC assessors for the conduct of CMMC assessments," states the Department of Defense on its website.

In the event a cyber incident occurs with a certified organization, the C3PAO may be asked to support the investigation. An organization's CMMC level and approval status should be considered confidential and should not be used for marketing purposes or made publicly available. Currently, compliance with cybersecurity requirements defined by DFARS 252.204-7012 only requires self-attestation. Validation by a C3PAO will provide the DoD with higher confidence that organizations are meeting the requirements.

A C3PAO is a service provider organization that Cyber-AB has accredited and authorized to conduct CMMC assessments and submits findings and certify that Organizations Seeking Certification (OSCs) comply with the CMMC 2.0. Contractor begins the assessment process by selecting a C3PAO to conduct their assessment.

Additionally, penetration testing and potentially other technical exercises, such as unannounced red teaming either performed by a third-party or requested to be performed and results provided, will be required for CMMC at the higher maturity levels. This will add another element that will help drive improved cybersecurity hygiene and will provide additional assurance over what is required today.

THE EVOLUTION OF 1.0 TO 2.0

So how Is CMMC 2.0 Different from the 1.0 Version?

Between 2020 and 2023, the DoD has introduced modifications in response to feedback on CMMC 1.0. Their goal was to minimize expenses and bureaucratic hurdles, especially for small businesses, enhance confidence in the CMMC evaluation framework, and better align cybersecurity requirements with other federal mandates and widely recognized standards.

The initial version of CMMC outlined five compliance maturity levels that range from Level 1 Basic Cybersecurity Hygiene to Level 5 Advanced Cybersecurity Practices. Each of the five levels outlines controls and processes that, when properly implemented, will reduce the risk of a breach to a company's cybersecurity defenses.

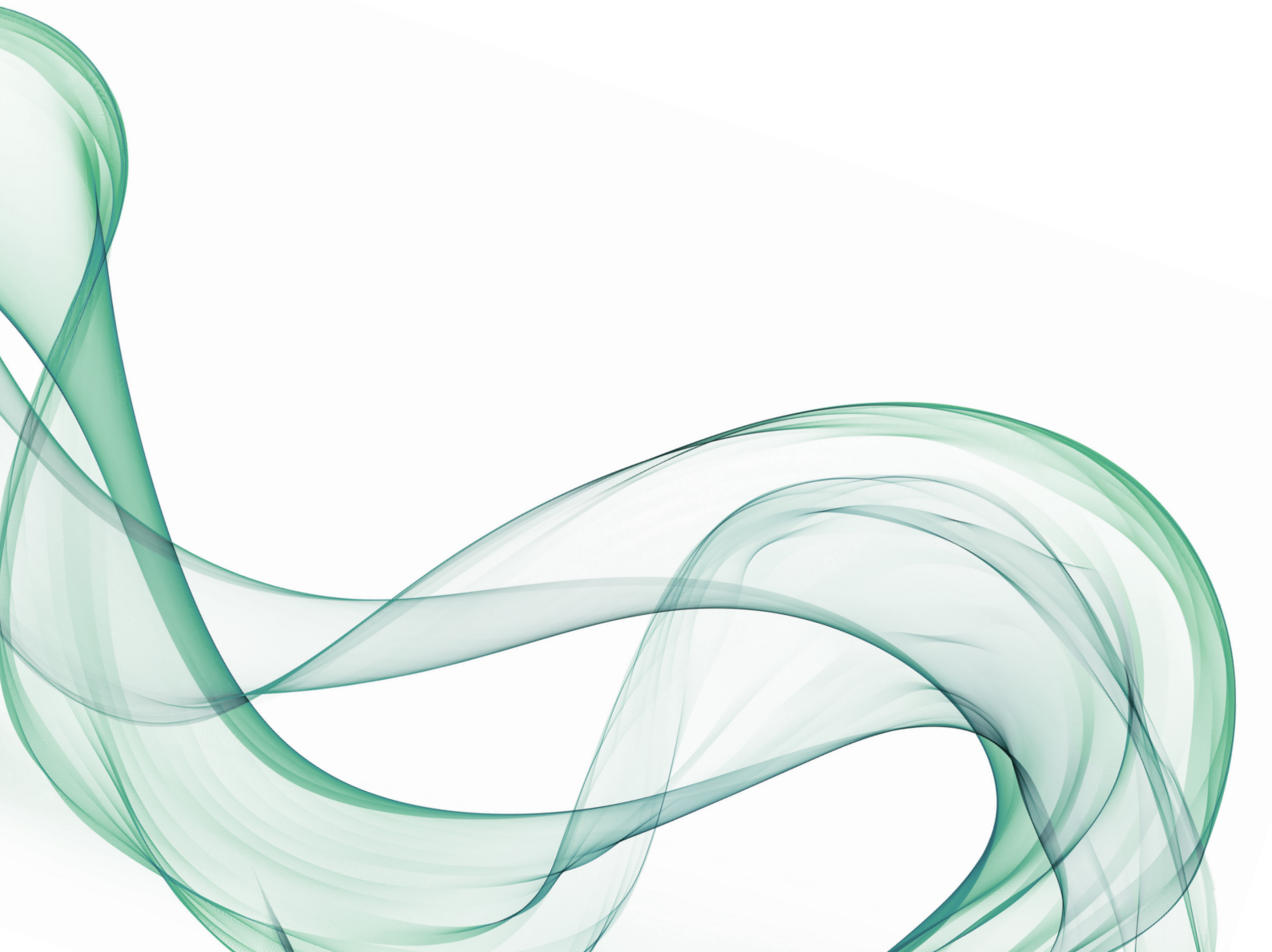
The levels are outlined below:

Level	Description of Practices	Description of Processes
Level 1 BASIC	• Basic cybersecurity • Achievable for small companies • Subset of universally accepted common practices • Limited resistance against data exfiltration • Limited resilience against malicious actions	Practices are performed, at least in an ad hoc manner
Level 2 INTERMEDIATE	• Inclusive of universally accepted cybersecurity best practices • Resilient against unskilled threat actors • Minor resistance against data exfiltration • Minor resilience against malicious actions	Practices are documented
Level 3 GOOD	• Coverage of all NIST SP 800-171 Rev 1 controls • Additional practices beyond the scope of Controlled Unclassified Information (CUI) protection • Resilient against moderately skilled threat actors • Moderate resistance against data exfiltration • Moderate resilience against malicious actions • Comprehensive knowledge of cyber assets	Processes are maintained and followed
Level 4 PROACTIVE	• Advanced and sophisticated cybersecurity practices • Resilient against advanced threat actors • Defensive responses approach machine speed • Increased resistance against and detection of data exfiltration • Complete and continuous knowledge of cyber assets	Processes are periodically reviewed, properly resourced, and improved across the enterprise
Level 5 ADVANCED	• Highly advanced cybersecurity practices • Reserved for the most critical systems • Resilient against the most advance threat actors • Defensive responses performed at machine speed • Machine-performed analytics and defensive actions • Resistant against, and detection of, data exfiltration • Autonomous knowledge of cyber assets	Continuous improvement across the enterprise

In November 2021, the Department announced "CMMC 2.0," an updated program structure and requirements designed to achieve the primary goals of the internal review:

- Safeguard sensitive information to enable and protect the warfighter
- Enforce DIB cybersecurity standards to meet evolving threats
- Ensure accountability while minimizing barriers to compliance with DoD requirements
- Perpetuate a collaborative culture of cybersecurity and cyber resilience
- Maintain public trust through high professional and ethical standards

CMMC 2.0 differs from the 1.0 version in three main ways: the reduction of maturity levels, changes to assessment requirements, and contract provisioning.



Streamlined Maturity Model

In CMMC 2.0, the number of maturity levels has been streamlined from five to three, eliminating Levels 2 and 4 from the previous version. The three new levels in CMMC 2.0 directly correlate to existing federal requirements: Level 1 (Foundational), Level 2 (Advanced), and Level 3 (Expert).

Assessment Requirements

Assessment requirements have also been modified in CMMC 2.0. Currently, Level 1 contractors can now perform annual self-assessments, while Level 2 contractors can complete self-assessments and submit senior official affirmations for non-prioritized acquisitions or require third-party assessments for prioritized acquisitions. Level 3 contractors must undergo triennial CMMC certification conducted by government officials. Subject to the rule making process, the above self-assessment process may be modified for Level 2 suppliers.

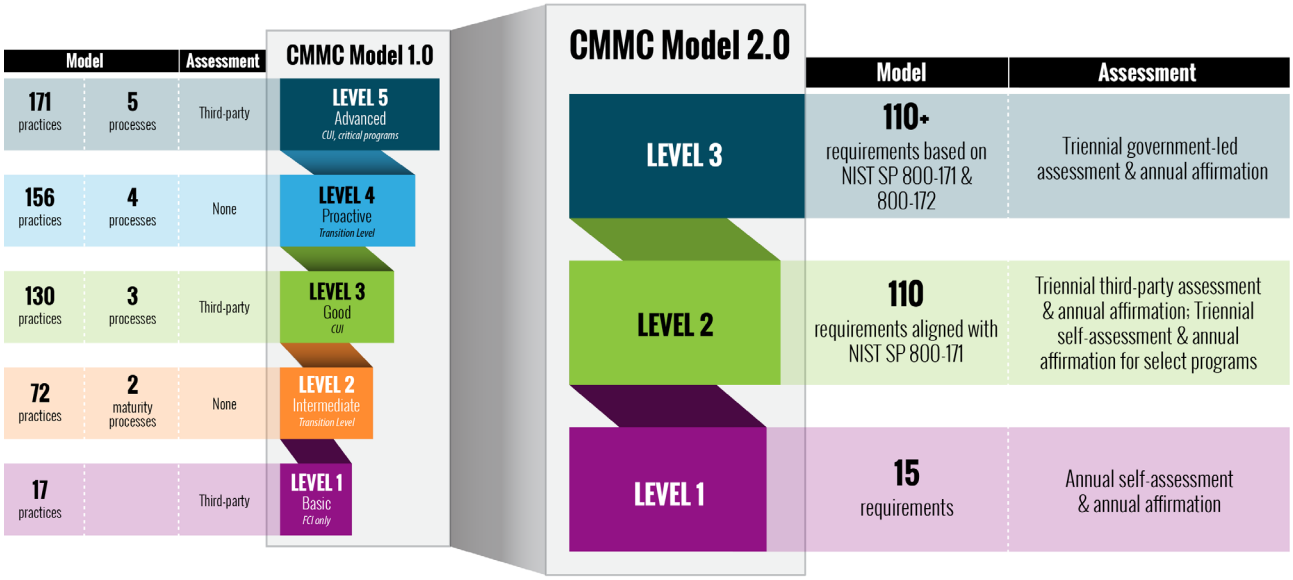
Implementation through Contracts

Once CMMC is fully implemented, certain DoD contractors that oversee sensitive unclassified DoD information will be required to achieve a particular CMMC level as a condition of contract award.

According to the Chief Information Officer Department of Defense page, the model of 2.0 varies per their diagram below.

Key Features of CMMC 2.0

**** Comparison between CMMC Models 1.0 and the planned CMMC Model 2.0. The CMMC Model 2.0 is notional until rulemaking is completed. ****



CMMC 2.0 APPLICABILITY

The requirement for CMMC 2.0 compliance will begin rolling out in the DoD contracts as early as Q1 2025. At that time, CMMC is not expected to be retroactively required of existing contracts or their options years. It will, however, apply to not only prime contract awardees but also to all subcontractors and, eventually, all solicitations including Requests for Information (RFIs) and Requests for Proposals (RFPs). The CMMC Level will be outlined in either Section L or M and will be a Pass/Fail compliance requirement.

The Office of the Under Secretary of Defense for Acquisition and Sustainment [OUSD (A&S)] has indicated that every company within the DoD supply chain, which comprises approximately 365,000 contractors and subcontractors, will eventually need to get certified at a CMMC level to contract with the DoD.

Recertification will be required at least every three years, and it could be determined in future guidance that recertification is required more frequently at Maturity Level 3 Previously, compliance

requirements related to DFARS 252.204-7012 and NIST SP 800-171 were only required for those who stored and/or processed CUI. As CMMC 2.0 is rolled out to new contracts, every contractor, subcontractor, and/or supplier for the DoD will eventually be expected to receive a certification at one of the three levels outlined in the table above. Higher risk contracts/programs will require a higher level of CMMC Maturity (Level 3), with Level 1 being the minimum for any organization storing and/or processing FCI. Organizations managing CUI will need to obtain Level 2 certification.

Without the required level of certification for a particular solicitation, organizations will be deemed non-compliant and therefore not eligible to compete.

Level Breakdown for CMMC 2.0

Level 1: Basic Cybersecurity

- Comprises 17 essential cybersecurity practices.
- Requires an annual self-assessment.
- Aimed at contractors dealing with Federal Contract Information (FCI).

Level 2: Advanced Cybersecurity

- Incorporates 110 practices based on NIST SP 800-171.
    - A key change from CMMC 1.0 is the reduction of practices to 110 from the previous 130. Focuses on companies managing Controlled Unclassified Information (CUI), Controlled Technical Information (CTI), and ITAR data.
- Requires third-party assessments by Certified CMMC Third-party Assessment Organizations (C3PAO).

Level 3: Expert Cybersecurity

- Involves 110+ practices, including new standards from NIST SP 800-172.
- Geared towards organizations that manage secret or top-secret information.
- Requires third-party assessments by Certified CMMC Third-party Assessment Organizations (C3PAO).

Who Does CMMC 2.0 Affect?

Target Groups

- Contractors supporting the Department of Defense
- Higher education research institutions dealing with data like:
    - Federal Contract Information (FCI)
    - Controlled Unclassified Information (CUI) / Covered Defense Information (CDI)
    - Controlled Technical Information (CTI)
    - International Traffic in Arms Regulations (ITAR) Data

WHY IS THIS MODEL AND UPDATES NEEDED?

"CMMC 2.0 will dramatically strengthen the cybersecurity of the defense industrial base," said Jesse Salazar, Deputy Assistant Secretary of Defense for Industrial Policy. "By establishing a more collaborative relationship with industry, these updates will support businesses in adopting the practices they need to thwart cyber threats while minimizing barriers to compliance with DoD requirements."

The below are examples, both when this white paper was originally published and now, of how clandestine, attacks are evolving based on data provided by the Center for Strategic and International Studies (CSIS):

THEN:

December 2018: U.S. Navy officials reported that Chinese hackers had repeatedly stolen information from Navy contractors, including ship maintenance data and missile plans.

July 2019: The U.S. Coast Guard issued a warning after receiving a report that a merchant vessel had its networks disrupted by malware while traveling through international waters.

August 2019: Chinese state-sponsored hackers were revealed to have targeted multiple U.S.-based cancer institutes to take information relating to innovative cancer research.

NOW:

March 2023: CISA and FBI reported that a U.S. federal agency was targeted by multiple attackers, including a Vietnamese espionage group, in a cyberespionage campaign between November 2022 and January 2023. Hackers used a vulnerability in the agency's Microsoft Internet Information Services (IIS) server to install malware.

June 2023: Several U.S. federal government agencies, including Department of Energy entities, were breached in a global cyberattack by Russian-linked hackers. Cybercriminals targeted a vulnerability in software that is widely used by the agencies, according to a US cybersecurity agent.

July 2023: Chinese hackers breached the emails of several prominent U.S. government employees in the State Department and Department of Commerce through a vulnerability in Microsoft's email systems.

Regardless of whether an organization provides operations, services, or performs maintenance for a DoD facility, it may have detailed information about building schematics, covered unclassified information or in some cases where maintenance is provided, underground utilities and electric grid information. This information in the wrong hands could be used to do harm, so the DoD must have assurance of its protection.

WHY IS THIS MODEL AND UPDATES NEEDED?

CMMC 2.0 leverages multiple frameworks, incorporating NIST SP 800-171r2, NIST SP 800-171, NIST SP 800-172, DFARS 252.204-7012 Clause, NIST CSF, ISO, and CIS as supportive detail. The most crucial step is to become familiar with the security requirements outlined in the model. A baseline assessment is highly recommended.

Organizations mandated to comply should undertake several crucial actions:

- Gain a comprehensive understanding of the model's security requirements.
- Conduct a baseline assessment and identify potential gaps.
- Include a network assessment and vulnerability assessment
- Determine the level of DoD data stored/processed to ascertain the applicable compliance level.
- Engage in a thorough, fact-based gap analysis.Develop processes, procedures, and incident response plans for compliance.
- Identify all weaknesses and threats to your organization and build a plan to remediate them.
- Prepare required documentation and enable monitoring capabilities for new threats and changes.
- Proactively consider future solicitations to align compliance levels.

Times to meet compliance can be lengthy and starting early to understand the cyber posture baseline will pay dividends. The specific level to which a company is expected to comply will only be released in the contract solicitation process. Although some general preliminary guidelines have been disclosed publicly, they may be subject to change in the definitive version.

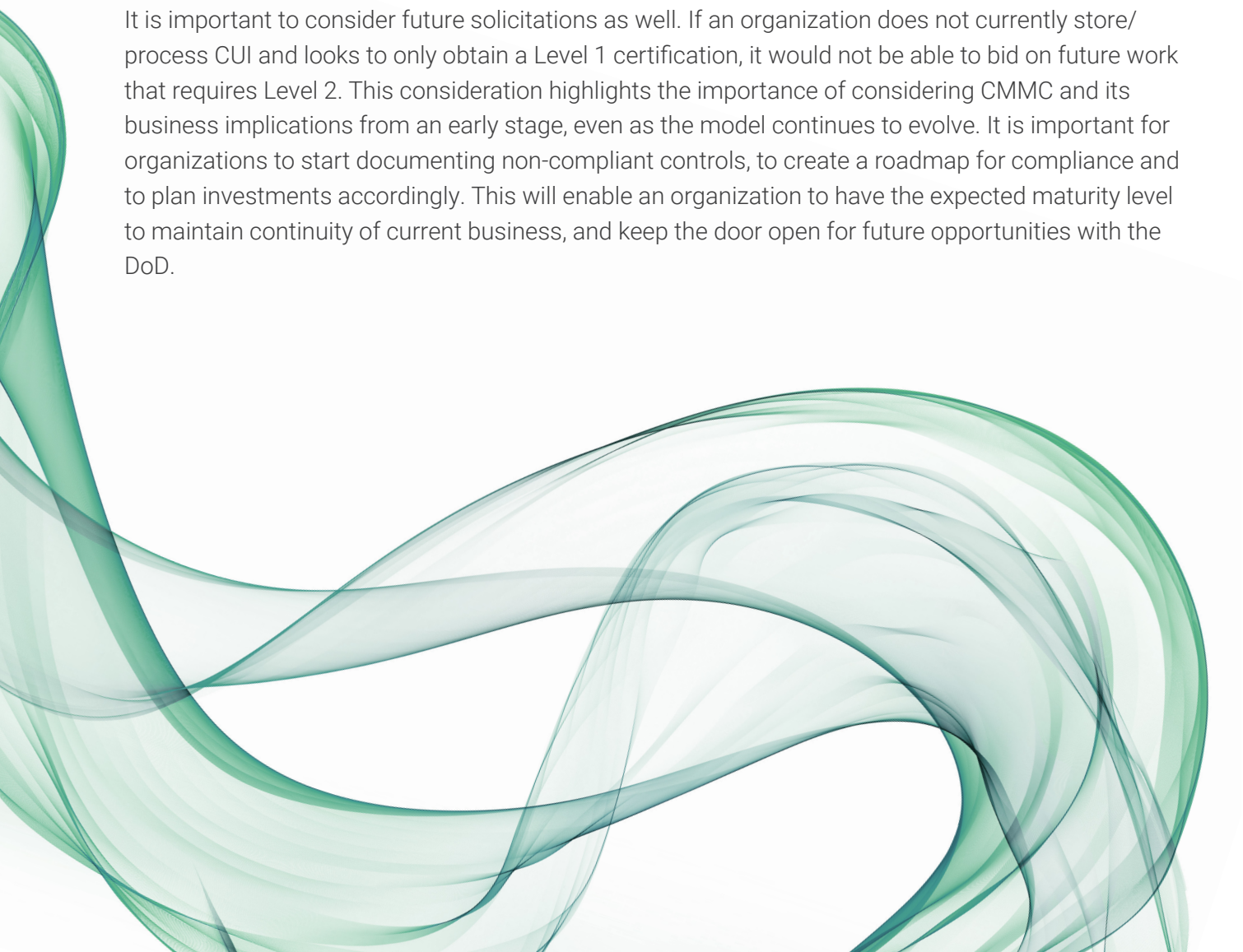
A company should target “Good Cyber Hygiene” as a best practice.

Guidelines include:

- Organizations without any DoD-specific data on their networks will be expected to comply with Level 1 or Level 2 requirements and undergo reassessment at least every three years.
- Organizations storing and/or processing CUI and thus previously required to comply with DFARS 252.204-7012 will correlate to CMMC Level 2, and undergo assessment at least every three years.
- Organizations with data related to critical infrastructure protection, such as warfighter designs, will be expected to comply with Level 3, potentially undergo assessment more frequently, and be subject to penetration testing.

After the model has been reviewed, organizations should determine the type of DoD data that is stored/processed on their networks to determine which level they will be expected to comply with. From there they can perform a thorough, fact-based gap analysis, prepare their required documentation, develop processes, procedures, enable monitoring capabilities and develop an incident response plan to comply with the reporting obligations.

It is important to consider future solicitations as well. If an organization does not currently store/process CUI and looks to only obtain a Level 1 certification, it would not be able to bid on future work that requires Level 2. This consideration highlights the importance of considering CMMC and its business implications from an early stage, even as the model continues to evolve. It is important for organizations to start documenting non-compliant controls, to create a roadmap for compliance and to plan investments accordingly. This will enable an organization to have the expected maturity level to maintain continuity of current business, and keep the door open for future opportunities with the DoD.



WHAT ARE THE PENALITIES FOR NON-COMPLIANCE?

Prior to CMMC, the government had some leverage in using the False Claims Act (FCA) to file lawsuits and levy fines. The appetite for Congress right now is very much about who is accountable for the exfils [exfiltration]." Examples of contractors who were fined due to FCA violations caused by intentional misrepresentation of organizations' security postures, including a fine of $4.9 million. With CMMC, the penalty is much higher—simply stated, an organization will not be able to do business with the DoD without the appropriate level of certification.

Since the Department of Defense (DoD) has formally presented the CMMC regulation for official evaluation, marking the start of its journey towards formal announcement. The subsequent stages of the rulemaking procedure are underway. Due to the intricate nature of federal rulemaking, several more stages need to be navigated before the CMMC becomes a part of contracts.

I. Scenario 1: Proposed Rule

a. Submission to OIRA: The Department of Defense (DoD) has officially submitted the CMMC rule for regulatory review to the Office of Information and Regulatory Affairs (OIRA).
b. Review and Publication: After OIRA's review, which takes an average of 66 business days, the **CMMC rule is expected to be published in late October 2023**.
c. Public Comment Period: A standard 60-day public comment period will follow, ending in December 2023.
d. Finalization: The CMMC rule will be published as a "proposed rule", which means it will only become effective after the agency responds to public comments in a final rule. Based on historical data, the average time for DoD proposed rules to be published as final rules is 333 business days. **This means the CMMC final rule is expected between February and April 2025.**
e. Phased Roll-Out: The DoD plans a 3-year phased roll-out for CMMC contract clauses. Assuming the final rule is published in Q1 2025, all relevant DoD contracts will contain CMMC by 2028.

II. Scenario 2: Interim Final Rule

a. Immediate Effectiveness: *If the CMMC rule is published as an "interim final rule", it will be effective before the agency responds to public comments.* **This means the rule would be in effect and appear in contracts in Q1 2025.**
b. Rarity of Interim Final Rules: Such rules are rare and bypass the usual democratic process of "notice and comment" rulemaking. They are typically granted in urgent situations, like the need to enhance national security.

CONCLUSION

CMMC 2.0 represents a pivotal advancement in the DoD's cybersecurity endeavors, reinforcing the defense against evolving threats. Organizations must proactively embrace CMMC 2.0, ensuring alignment with the refined security requirements and strategic considerations. By adhering to the new model, entities can effectively secure their place within the DoD supply chain, safeguard national defense interests, and contribute to the collective effort of cybersecurity enhancement.

The CMMC effort has been a significant, but necessary change in the DoD acquisition process and will provide overall improvement in securing the DIB and its supply chain. Interpreting and implementing the requirements can be achieved with thoughtful planning, preparation, and resources, especially for organizations that have already undertaken efforts to follow DFARS 252.204-7012.

All organizations working for and with the DoD will need to start the process working with the new security requirements and evaluate their strategy to comply. For organizations to begin or continue to do business with the DoD, it will be critical for them to identify potential gaps, establish a timeline for completion, and secure the right organizational resources and technologies to enable a rapid implementation of the new model.

Best Practices to Consider

1. Framework-based assessment of controls, assets, and cyber-risks
2. Define a plan to resolve and monitor high risks.
3. Implement a cyber-risk management program that has a defense in depth methodology.
4. Consider Managed Service Providers with a holistic risk, threat and respond approach to compliance management.

cytellix.com

info@cytellix.com

(949) 215-8889