



CYBERSECURITY MATURITY MODEL CERTIFICATION

A FEDERAL CONTRACTOR'S GUIDE TO CMMC 2.0

Oct 2023

Index

1. EXECUTIVE SUMMARY	03
2. BACKGROUND AND CONTEXT	05
• What is NIST 800-171?	05
• Why did NIST 800-171 fall short?	05
• Evolution of CMMC and Rule-making	06
• CMMC Vs. NIST SP 800-171	08
3. CMMC 2.0 FRAMEWORK	09
• How many domains and practices does CMMC 2.0 have?	10
• Why is CMMC compliance important?	10
• Who does CMMC apply to?	12
• Navigating Prime and Subcontractor CMMC Responsibilities amidst new regulations	12
4. THE CMMC ECOSYSTEM	14
• Attack Surfaces in the Defense Supply Chain	15
5. CMMC: FROM READINESS TO CERTIFICATION	17
• What CMMC level do I need?	17
• When will CMMC requirements start appearing in solicitations?	17
• How long does it take to get CMMC certified?	17
• What does the journey to CMMC certification look like?	19
• What are the challenges faced by small businesses to comply with CMMC?	19
• What are the CMMC 2.0 assessment requirements?	21
• How much does CMMC Compliance Cost?	21
6. FAQ'S	23
• What are some of the most challenging controls to implement?	23
• What is the difference between Basic, Medium, and High assessments?	23
• Which controls are consistently failing DIBCAC assessments?	24
• What is SPRS?	24

• Are POA&Ms allowed in CMMC 2.0?	25
• Are waivers allowed in CMMC 2.0?	25
• Will prime contractors and subcontractors be required to maintain the same CMMC level?	26
• Will my organization need to be certified if it does not handle CUI?	26
• Who oversees CMMC within a company: the FSO or the IT director?	26
• Will my assessment outcomes be accessible to the public and the DoD?	26
• How should a company handle situations where complete CMMC implementation interferes with necessary system functionality?	26
• What are the 17 CMMC Domains?	27
7. HOW CAN AN RPO HELP IN CMMC COMPLIANCE?	29
• Case Study 1 : Unleashing cybersecurity success	30
• Case Study 2 : Accelerating CMMC compliance	31
8. APPENDIX	32
• CMMC Glossary	32

Executive Summary

Welcome to an updated and our most comprehensive guide on Cybersecurity Maturity Model Certification (CMMC) 2.0!

The CMMC is a program spearheaded by the U.S. Department of Defense (DoD) aimed at safeguarding Controlled Unclassified Information (CUI) by ensuring that organizations have the necessary cybersecurity measures in place to prevent unauthorized access, usage, or dissemination of sensitive data.

The latest iteration, CMMC 2.0, brings forth a tiered system spanning levels from 1 (Basic Cybersecurity Hygiene) to 3 (Advanced/Progressive), helping entities to categorize and manage cybersecurity with a perspective aligned to their risk management strategies and business needs.

As we navigate through a landscape where cyber threats are constantly evolving and getting sophisticated, **being CMMC compliant not only stands central to securing an organization's assets and data but is also pivotal in fostering credibility and gaining a competitive edge in the marketplace.**

In July 2023, the Department of Defense (DoD) formally presented the CMMC 2.0 rule to the Office of Information and Regulatory Affairs (OIRA), an agency overseen by the Office of Management and Budget (OMB). This submission initiated a systematic regulatory review process, laying the groundwork for the rule's official implementation.

Following this, there is an anticipation of a defined timeline, with the rules potentially being published by late October 2023, marking the onset of a 60-day public comment period expected to close in December 2023.

What does this mean for organizations in the defense sector? The journey toward CMMC certification will soon be more than just a strategic step; it will become a mandatory requirement for all DoD contractors. There has already been a significant uptick in CMMC requirements in the solicitations this year. **Once the rule-making is finalized, these requirements in the solicitation will expand exponentially over the next few years.**

Businesses, especially small enterprises, are encouraged to gear up for this change by understanding the CMMC level pertinent to them and initiating the necessary steps toward certification. **It is vital to undertake this journey with foresight, factoring in the time, which can range anywhere from a few months to a couple of years depending on various dynamics, such as the complexity of your organization and the level of certification you are targeting.**

Engaging with professional consulting firms can aid in delineating a path that is in alignment with your budget and needs, helping you to navigate the complexities with ease.

As the final rule is anticipated to be in effect between Q1 2024 and Q1 2025, with a phased rollout spanning three years, starting your preparations now will ensure a smooth transition, helping you to uphold the integrity of sensitive information while reaping the manifold benefits of CMMC compliance.

This guide will delve into these topics and more to provide you with a comprehensive understanding of CMMC 2.0 and the importance of achieving compliance.

In 2022, DoD released a [memorandum](#) that stated:

The protection of controlled unclassified information on contractor information systems is critically important to the Department of Defense (DoD).

To that end, [Defense Federal Acquisition Regulation Supplement \(DFARS\) clause 252.204-7012](#), "Safeguarding Covered Defense Information and Cyber Incident Reporting," requires contractors to provide adequate security on all covered contractor information systems, defined as an unclassified information system owned or operated by or for a contractor, and that processes, stores, or transmits protected defense information.

Adequate security measures include, as applicable, implementation of the security requirements in the [National Institute of Standards and Technology \(NIST\) Special Publication \(SP\) 800-171](#), "Protecting Controlled Unclassified Information in Non-federal Information Systems and Organizations" in effect at the time the solicitation is issued or as authorized by the contracting officer.

Background and Context

What is NIST 800-171?

The Department of Defense (DoD) mandated in the early 2018 that all organizations exchanging CUI enforce the 110 security controls listed in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 (NIST 800-171): [Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations](#).

However, despite the existence of this regulation, CUI leakage persisted, endangering American national security.

Why did NIST 800-171 fall short?

The core reason why NIST 800-171 compliance was insufficient is that it relied on self-assessments.

But why was it problematic? Here are a few reasons:

1. Security Controls are complex.

The security controls are complex, and the organization implementing or assessing themselves can easily misunderstand all requirements and incorrectly value their assessments.

2. Questionable Self-Assessment processes.

Due to subjectivity, self-assessments are usually not regularly, comprehensively, and consistently performed at organizations, which decreases the reliability and validity of the self-assessment.

3. 100% Compliance with NIST standards doesn't guarantee 100% cyber protection.

Complying with NIST 800-171 does not necessarily mean that security is ensured at the company. Even if the organization satisfies a security control requirement, it needs to address the strength and maturity utilized to fulfill the requirement.

To overcome the shortcomings in NIST 800-171 compliance enforcement, and the need to continually defend the vast attack surface of the Defense Industrial Base (DIB), the DoD released a tiered system of Cybersecurity Maturity Framework in 2020.

Evolution of CMMC and Rule-making

2015-2020

The journey began with the release of NIST Special Publication 800-171 in 2015, a guideline developed to fortify the protection of Controlled Unclassified Information (CUI) in non-federal systems. To enforce this, the DoD introduced [DFARS clause 252.204-7012](#), requiring the Defense Industrial Base (DIB) to adhere to NIST 800-171 controls through self-attestations. The phase also saw the establishment of the CMMC 1.1 framework in 2020 to enhance data safeguarding measures surrounding CUI and FCI data.

2021-Present

Criticisms regarding the complexity and projected certification costs of the initial CMMC version ushered in CMMC 2.0 in November 2021, aiming to create a more accessible compliance pathway for smaller firms without compromising the defense industrial base's cybersecurity.

As of July 2023, the CMMC rule-making has reached a significant milestone, with the DoD submitting the draft to the Office of Information and Regulatory Affairs (OIRA). The next probable steps entail the following:

1. OIRA's regulatory review is expected to conclude by October, 2023.
2. Public commentary and review by December, 2023.
3. Ratification of the rule-making and thus shaping the eventual incorporation of CMMC into contracts, tentatively by Q1 2025.
4. Publication in the Federal Register.

The Future

The CMMC landscape is poised for potential alterations based on OMB's decisions during the rule publishing – opting for a proposed rule, which is more likely, or choosing the less anticipated interim final rule.

The former scenario leads to a phased CMMC implementation from Q2-Q3 of FY 2025, post a 60-day commentary period, while the latter accelerates the incorporation to as early as Q1 of FY 2024. Industry insiders are closely watching the NIST's maneuvers, which are in the process of finalizing the SP 800-171 Revision 3, set to elevate cybersecurity controls further. This revision, anticipated to materialize between Q1 and Q2 of FY 2024, may provoke the DoD to grant a "class deviation."



Class Deviation

In the context of regulatory and compliance environments, "class deviation" refers to a temporary alteration or adjustment to a policy, standard, or regulation that applies to a specific group or "class" of entities, effectively extending the compliance deadline to synchronize with CMMC's potential FY 2025 implementation.

Given the active developments, firms are advised to advance their compliance with the existing NIST SP 800-171 standards to transition into the CMMC requirements smoothly. Initiating this now is prudent, considering the considerable time - typically a few months to 2 years - required to become assessment ready.

The enforcement of CMMC showcases the current administration's alignment with augmenting cybersecurity requisites in the defense contracting landscape, reflecting a paradigm shift in national cybersecurity strategy.

Staying updated on further announcements, such as the status of the Joint Surveillance Voluntary Assessment (JSVA) program and the new DFARS Interim Rule disclosures, which herald the legal embedding of CMMC through the anticipated DFARS 7021 clause, is essential.

Type of Rule	Definition	Purpose
Proposed Rule	A draft version of a rule published in the Federal Register to notify the public and solicit comments.	To collect public input and allow stakeholders to provide feedback before the rule is finalized.
Interim Final Rule	A rule issued without a proposed rule stage but is open to public comment after issuance. It might be modified based on the feedback received.	To hasten the rule-making process in urgent situations while still offering a period for post-issuance public comment.
Current Interim Rule	Potentially referring to an interim rule that is currently in effect, serving as a provisional rule before the final rule is established.	To provide a temporary regulatory framework in urgent situations or when immediate changes are necessary while the formal rule-making process is underway.
Final Rule	The officially adopted and implemented version of a rule becomes legally binding once published in the Federal Register.	To enact a legally binding rule incorporating feedback from previous stages and finalize the regulatory framework.

Exhibit 1: The Federal Rulemaking Definition



Federal Contract Information (FCI)

Information not intended for public release. It is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government. FCI does not include information provided by the Government to the public.



Controlled Unclassified Information (CUI)

Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

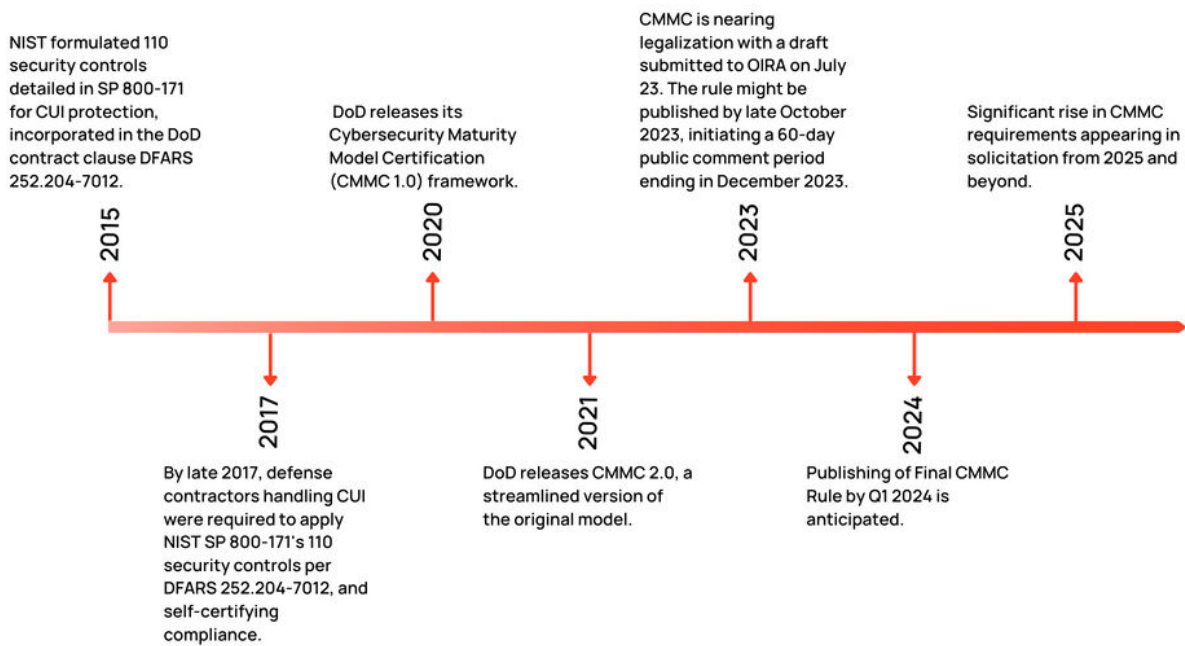


Exhibit 2: CMMC Rulemaking Timeline

CMMC And NIST SP 800-171 Comparison

Aspect	CMMC	NIST SP 800-171
Purpose	Assess and enhance the cybersecurity posture of the defense industrial base (DIB).	Provide guidelines for protecting Controlled Unclassified Information (CUI) in non-federal systems and organizations.
Developed By	Department of Defense (DoD)	National Institute of Standards and Technology (NIST)
Scope	Covers 3 cybersecurity maturity levels, from basic cyber hygiene to advanced.	Focuses on the protection of CUI in non-federal systems and organizations.
Levels/Maturity	3 levels, ranging from basic cyber hygiene to advanced cybersecurity practices.	Operates based on a set of 110 controls/recommendations.
Certification Process	Organizations need to undergo evaluations by third-party assessors (C3PAOs) to earn certifications.	Self-assessment is generally allowed, but organizations need to implement the specified controls.
Applicability	Primarily targeted at defense contractors and subcontractors in the DIB.	Intended for non-federal organizations and contractors in the DIB.
Verification of Compliance	Requires third-party assessment for verification.	Generally self-assessed, but third-party assessments can be opted to verify compliance.
Flexibility & Implementation	Less flexible, it demands compliance with a predefined set of controls at each level.	Offers flexibility in implementation, allowing tailoring based on specific needs and circumstances.
Adoption	Mandated for all DoD contractors and subcontractors through a phased rollout.	Adopted by various Non-Federal organizations, including the DoD Supply chain, before the introduction of CMMC.

Exhibit 3: NIST Vs CMMC

Cybersecurity Maturity Model Certification 2.0 Framework

CMMC, created to defend the defense industrial base (DIB) from increasingly frequent and sophisticated cyberattacks, specifically intends to improve the security of federal contract information (FCI) and controlled unclassified information (CUI) transferred within the DIB.

CMMC compliance aims to assess defense contractors' capabilities, readiness, and sophistication in cybersecurity. The framework comprises processes and other frameworks and inputs from cybersecurity standards like NIST 800-53, ISO 27001, UK Cyber Essentials, and Australia Cyber Security Centre Essential Eight Maturity Model. The program is designed to help federal contractors improve their cybersecurity posture through a standardized maturity model.

As threats change, CMMC 2.0 expands on the original CMMC 1.0 framework to dynamically improve DIB cybersecurity. The CMMC framework ensures accountability, safeguards critical unclassified information shared by the DoD, and reduces obstacles to compliance with DoD regulations. Three levels based on well-recognized NIST cybersecurity standards have replaced the five cybersecurity compliance levels in CMMC 1.0.

With the implementation of the Cybersecurity Maturity Model Certification (CMMC) 2.0 program, the Department is introducing several key changes that build on and refine the original program requirements.

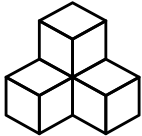

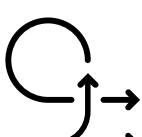
	<p>Streamlined Model</p>	<p>Focused on most critical requirements: Streamlines the model from 5 to 3 compliance levels</p> <p>Aligned with widely accepted standards: Uses National Institute of Standards and Technology (NIST) Cybersecurity standards</p>
	<p>Reliable Assessments</p>	<p>Reduced Assessment costs: Allow all companies at Level 1, and a subset of companies at Level 2, to demonstrate compliance through self-assessment</p> <p>Higher Accountability: Increases oversight of professional and ethical standards of third-party assessors</p>
	<p>Flexible Implementation</p>	<p>Spirit of collaboration: Allow companies, under certain limited circumstances, to make Plans and Action & Milestones (POA&Ms) to achieve certification</p> <p>Added flexibility and speed: Allows the Government to waive the inclusion of CMMC requirements under certain limited circumstances</p>

Exhibit 4 : Simplified CMMC 2.0

How many domains and practices does CMMC 2.0 have?

- **Level 1 (Performed: 15 practices)** To protect Federal Contract Information, a company must follow fundamental cyber hygiene procedures, requiring employees to change passwords frequently. This level includes an annual self-assessment and an annual affirmation.
- **Level 2 (Managed: 110 practices)** To protect CUI, a company needs to have a standardized management strategy that includes all the NIST 800-171 r2 security requirements and procedures. This level contains a triennial third-party assessment and an annual affirmation.
- **Level 3 (Optimizing: 110+ practices)** A company needs to implement standardized, optimized processes and extra, improved practices that can identify and react to evolving advanced persistent threats (APTs). This level includes a triennial government-led assessment and an annual affirmation.

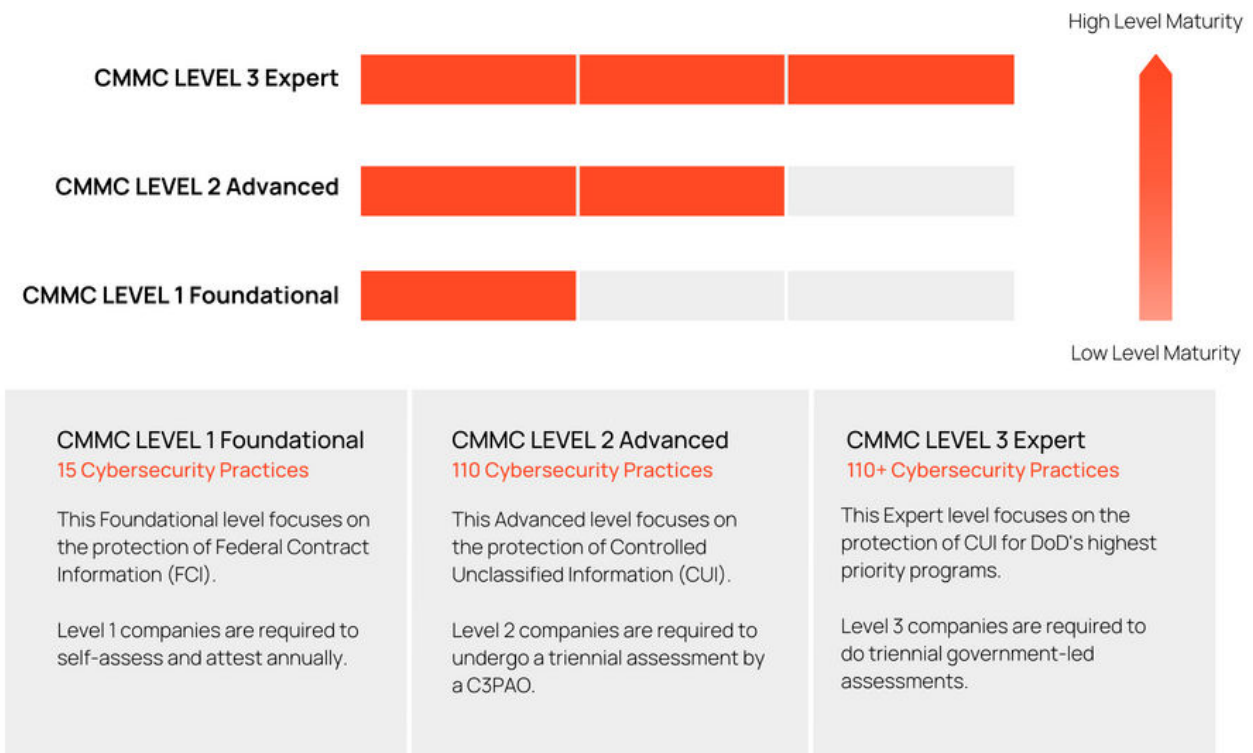


Exhibit 5. CMMC 2.0: Levels and Practices

Why is CMMC compliance important?

The significance of CMMC connects back to the United States' national security. The Defense Industrial Base (DIB) is a global industrial compound to supports vital services and goods such as the design, manufacture, delivery, and maintenance of military weapons systems to satisfy the needs of the U.S. military.

The DIB supply chain comprises **more than 300,000 businesses that work for the DoD** under contract. Defense contractors must have their cybersecurity status inspected and confirmed by an impartial third party before signing a contract with the DoD. In addition to the complexity of what is at risk, studies show that the global cost of cybercrime is around **\$945 billion**, which is more than 1% of the global GDP. The Department of Defense is putting in maximum effort to reduce the costs and risks through CMMC.

Below are the benefits of complying with CMMC:

1. CMMC Compliance ensures protection of sensitive Information (FCI/CUI)

CMMC compliance is important because there is highly sensitive national information at risk. The Government requires contractors to practice set standards and regulations to strengthen the information's security. Specifically, suppose a company is dealing with Controlled Unclassified Information (CUI) or Federal Contract Information (FCI), in that case, the company must have CMMC compliance to protect the information. CMMC ensures that companies working with the Department of Defense meet security protocols and standards.

2. CMMC Compliance will soon be a requirement for DoD contractors

Once the rule-making is in effect, CMMC compliance will become a mandatory requirement for DIBs. The DIB Contractors will not be able to bid on DoD Contracts if they fail to comply with the appropriate CMMC Level.

3. To avoid penalties under The False Claim Act

Contractors who make false statements or representations about their compliance with CMMC standards in order to obtain or retain a contract with the DoD could be subject to civil penalties, fines, and exclusion from future government contracts.

4. Achieving CMMC compliance can provide many benefits to Federal Contractor

Achieving CMMC compliance can offer many benefits to organizations, including **increased credibility and competitiveness** in the market, **improved cybersecurity posture**, and **protection of sensitive information**. Therefore, it is important for the organizations that handle CUI to comply with CMMC.

5. Enforcement of DFARS 254.204 7012

The Department of Justice has launched a robust **Cyber-Fraud Initiative** to hold contractors accountable for their cybersecurity. **It is encouraging whistleblowers to come forward with False Claims**. It would increase the scrutiny, resulting in increased pressure on Defense Contractors to comply with CMMC.

Who does CMMC apply to?

CMMC is a requirement for all companies who want to work as a **contractor/subcontractors within the Defense Industrial Base supply chain.**

Everyone involved in the defense contract supply chain, including contractors who work directly with the DoD and subcontractors who work with primes to carry out or complete contracts, must abide by the CMMC.

It is important to note that **while CUI may not flow down to subcontractors, compliance to CMMC still does**, meaning whether you have CUI/FCI in your system or not, if you work with a DoD supplier, you are required to comply with CMMC Level 1 at the minimum.

Navigating Prime and Subcontractor CMMC responsibilities amidst new regulations

In light of the unfolding developments in the Cybersecurity Maturity Model Certification (CMMC) landscape, the defense contracting sphere is entering a pivotal period where stringent adherence to the newly emphasized standards is not just recommended but becoming mandatory.

Prime contractors find themselves with heightened responsibilities as the Department of Defense (DoD) elevates its security requisites, impacting both the primes and their subcontractors significantly. Here is a detailed breakdown of the responsibilities and the anticipated shifts in the CMMC paradigm.

Prime Contractors Responsibilities

Ensuring Compliance

CMMC Certification: Prime contractors and their Tier 1 partners are urged to expedite their preparations for achieving the necessary CMMC certifications in readiness for the FY25 acquisition cycle.

Flow-down of DFARS 7012: Understanding that the DFARS 252.204 7012 clause often flows down reflexively, the primes should vigilantly assess the nature of the data being handled to determine the necessary security measures, including NIST SP 800-171 implementation.

Oversight and Management of Subcontractors

Active Monitoring:

The committee has raised concerns about the inadequate oversight of subcontractors, emphasizing the need for prime contractors to oversee the compliance levels of their subcontractors actively.

Accountability: The prime contractors are expected to be accountable for securing DoD technology and safeguarding sensitive information through the supply chain.

Exhibit 6: Prime Contractors Responsibilities

Subcontractors Responsibilities

Compliance with CMMC Standards

Preparedness: Subcontractors must work towards becoming “Assessment Ready,” a process that typically spans 3-24 months, to facilitate smooth CMMC Conformity Assessments when the time comes.

Engaging in Voluntary Assessments: DIBs who believe they are CMMC-ready should consider participating in Joint Surveillance Voluntary Assessments (JSVA) or engaging in NIST SP 800-171 assessments. To encourage DIBs to step forward and join in CMMC assessments, the JSVA incentivizes them to pass the assessment with a lower score of 88 versus the required 110 in the future. DIBs who pass the JSVA assessment will be eventually granted CMMC Level 2 certification in the future.

Response to Market Pressures

Proactiveness: Subcontractors should note the growing market pressures and act proactively to avoid revenue drop-offs and maintain a competitive edge in the business landscape.

Early Adoption: Primes are likely to insist on early certifications for their supply chains to stay ahead in compliance, setting a competitive benchmark in the industry.

Exhibit 7: Subcontractors Responsibilities

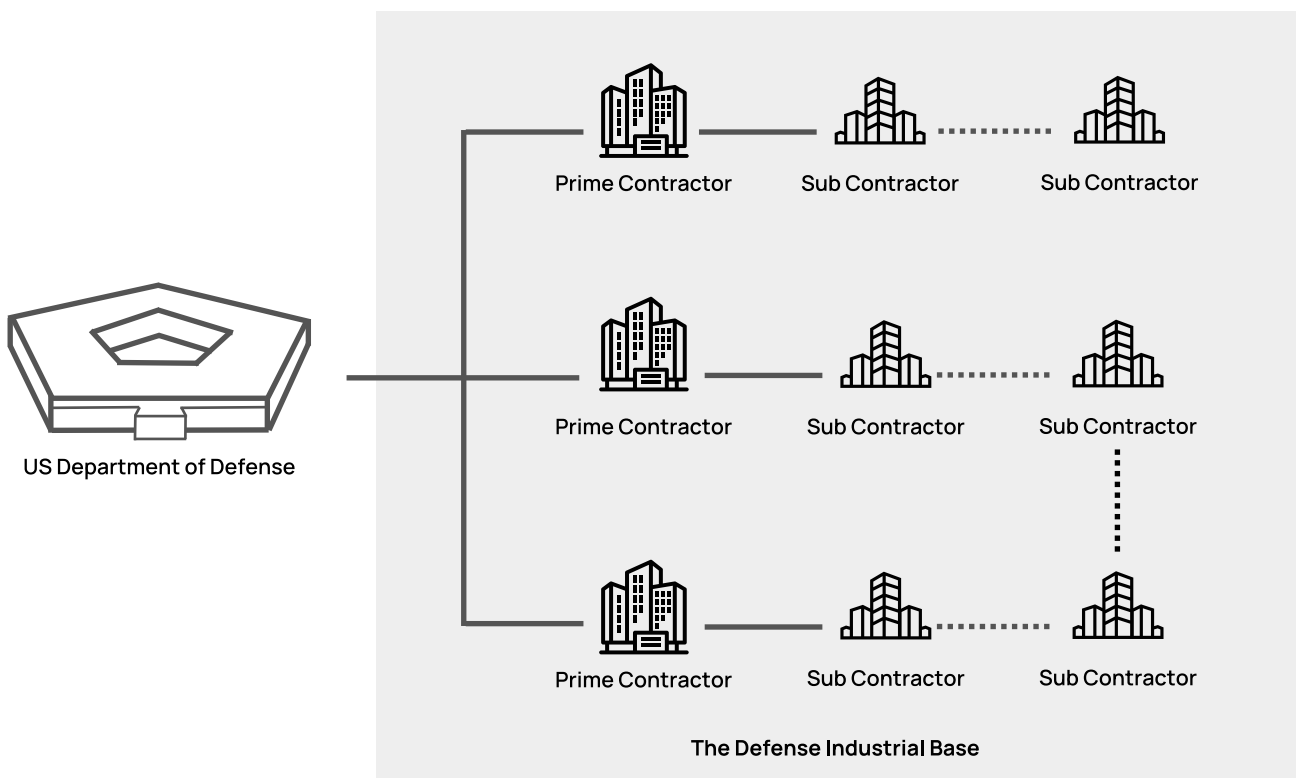


Exhibit 8: DIB Supply Chain

The CMMC Ecosystem

The CMMC Ecosystem has several stakeholders. Some of the most important are shown in the image below:

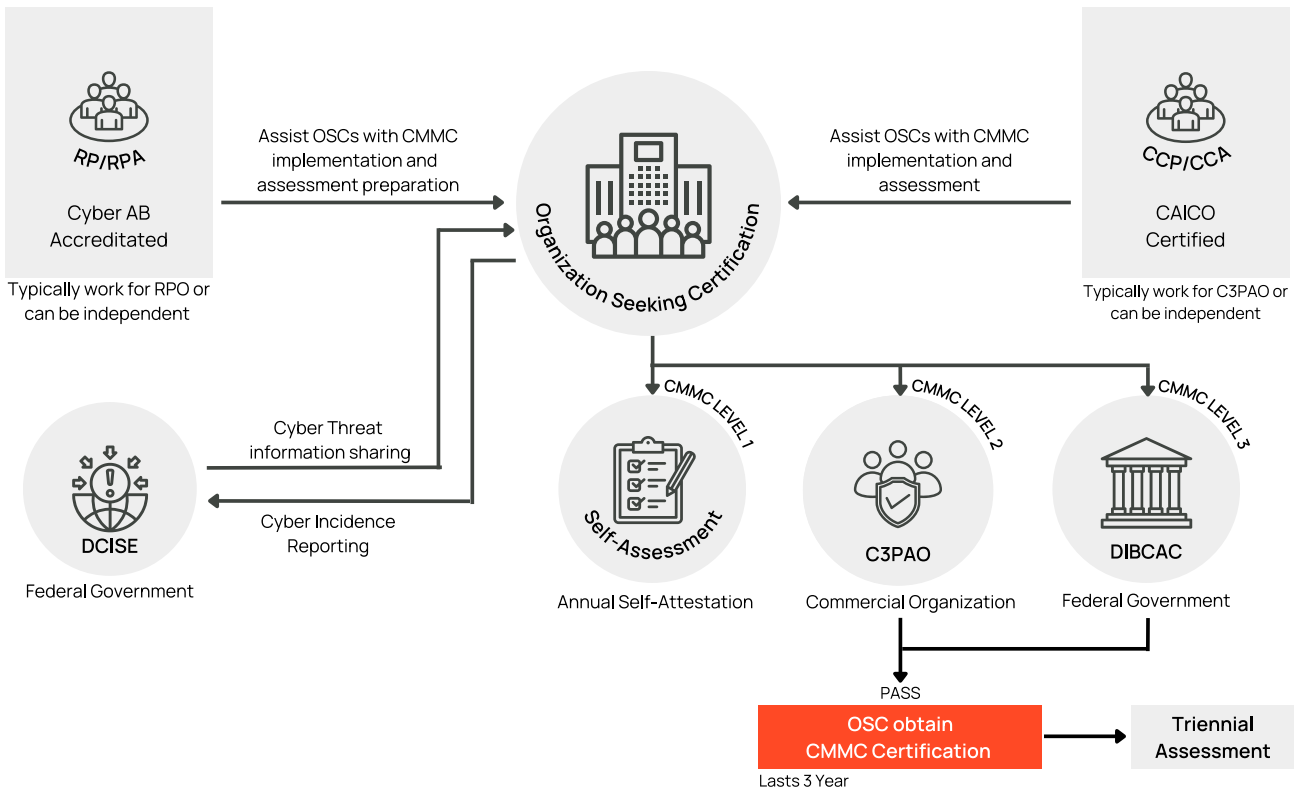


Exhibit 9 : The CMMC Ecosystem

- **OSC:** Organization Seeking Certification is any organization seeking any of the CMMC Level 1 to Level 3 Certification.
- **RP/RPA:** Registered Practitioners and Registered Practitioner Advanced, accredited by CyberAB, are implementers and IT solution architects that provide consultative preparation services to the OSCs and either work as independent contractors or as members of a Registered Practitioner Organization (RPO).
- **CCP/CCA:** Certified CMMC Professional (CCP for Level 1) or Certified CMMC Assessor (CCA for Level 2) are individuals who have received training from a Licensed Training Provider (LTP) and are required to take and pass the certification exams. On passing the certification exam(s), they become certified assessors. They typically work for a C3PAO or can be independent.
- **RPO:** CMMC RPOs provide pre-assessment consulting and remediation services to OSCs and assist them during assessments. They deliver advisory and consulting services through RP and RPAs. They are consultative organizations or MSPs and do not conduct Certified CMMC Assessments.

- **C3PAO**: A CMMC Third-Party Assessment Organization (C3PAO) conducts assessments of OSCs by employing CCPs and CCAs based on their training and adherence to CMMC standards.
- **DIBCAC**: DIBCAC is a federal agency that leads the Department of Defense's (DoD) contractor cybersecurity risk mitigation efforts. DIBCAC assesses DoD contractors' compliance with the Defense Federal Acquisition Regulation Supplement (DFARS), NIST (SP)800-171 clause, and other clauses.
- **DCISE**: Defense Industrial Base Collaborative Information Sharing Environment (DCISE) is the operational hub of the Defense Industrial Base (DIB) Cybersecurity Program of the Department of Defense, focused on protecting intellectual property and safeguarding DoD content residing on or transiting through contractor unclassified networks. The public-private cybersecurity partnership provides a collaborative environment for crowd-sourced threat sharing at unclassified and classified levels. Cyber incidents outlined in the DFARS are submitted by OSCs to DC3/DCISE as mandatory reports; however, all other cyber activity can be reported voluntarily:
 - Rated at the "Defined" level (Maturity Level 3) for Capability Maturity Model Integration for Services (CMMI-SVC) Oversees a collaborative partnership with over 1,003 CDCs and U.S. Government (USG) agencies. Has shared over 589,006 (and counting) actionable, non-submitting-source-attributable indicators.
 - Provides no-cost forensics and malware analysis for DIB Partners.
 - Disseminates cyber threat reports for both DIB and USG consumption (DIB partners access DCISE reporting via their DIBNET accounts, and USG members can access via SIPRNet Intelshare).
 - Operates a 24/7/365 support hotline (1-877-838-2174) to assist submitters and DIB and USG Partners.

Attack Surfaces in the Defense Supply Chain

In the defense industry, understanding and mitigating potential attack surfaces is imperative. As a Defense Contractor, being cognizant of these areas is vital:

Digital Infrastructure	The backbone of defense operations, Communication Channels, and Data Storage Systems are the most lucrative attack vectors for cyber adversaries often seeking to exploit vulnerabilities, introducing significant risks.
Third-Party Vendors	Vendors, or vendors of vendors in your network, can increase your attack surface exponentially. Each engagement with a vendor introduces new vulnerabilities, making this an essential area to monitor and manage to maintain operational security.

Personnel	Individuals, including employees and contractors, represent a potential attack surface, given the access they have to sensitive information. It is an area often exploited through techniques such as phishing and social engineering, requiring vigilant monitoring and management.
End-Point Devices	In the age of IoT, the number of end-point devices has proliferated, making them a hotspot for unauthorized access attempts and potential data breaches. Their ubiquitous presence marks them as a significant attack surface to be consistently overseen.
Physical Infrastructure	Beyond the digital landscape, physical infrastructures, encompassing the facilities that house essential assets and data, stand as potential attack surfaces. Ensuring the security of these spaces is crucial in the broader picture of safeguarding defense supply chains.
Managed Service Providers (MSPs)	An emergent concern is the role of MSPs. These entities hold substantial privileged access to regulated environments but remain largely under-regulated themselves. Recent drafts like the NIST SP 800-171 rev.3 have begun to highlight the potential threat vector represented by MSPs, flagging it as a prominent attack surface.

Exhibit 10: Attack Surfaces in DIB Supply Chain

The Road Ahead: Timeline and Expectations

While the official implementation of the new rule is anticipated to be either in mid to late 2024 or even early 2025, there is an undercurrent of urgency resonating in the sector, propagated largely by the prime contractors.

Besides that, a significant wave of conformity assessment requests is expected to flood C3PAOs, given the limited number of authorized bodies and qualified assessors to conduct the assessments. OSCs (Organizations Seeking Certifications) should remain cautious amidst the growing overhype, steering clear from misinformation and focusing on achieving compliance in a structured manner.

As the defense industrial base braces for the imminent CMMC tidal wave, it is incumbent upon businesses at every tier of the supply chain to foster a culture of readiness and vigilance. It is a critical juncture where preparation and early adoption of the CMMC norms can potentially delineate the leaders from the laggards in securing DoD contracts in the future.

Thus, it is more prudent than ever for organizations to kickstart their journey toward CMMC certification, beginning with a robust NIST SP 800-171 implementation.

CMMC: From Readiness to Certification

What CMMC level do I need?

According to DoD, there are approximately 300,000 organizations that would require CMMC. **There are about 80,000 organizations that would require CMMC Level 2 and Level 3, and the rest would require CMMC Level 1 compliance.**

To qualify for government contracts, most businesses will need certification between one of the three levels. The Department of Defense is working with the CMMC Accreditation Body (Cyber-AB) to enforce the process, ensuring the validity and certifying independent third-party assessment organizations (C3PAOs).

The level necessary depends on whether the company is dealing with CUI or FCI. FCI would require the company to complete Level 1, and dealing with CUI would require the company to have achieved Level 2.

When will CMMC requirements start appearing in solicitations?

CMMC requirements could appear in solicitations as early as Q1 2024. Since CMMC compliance is a long journey, currently, DoD allows you to bid on contracts.

However, in the future, the Government will only allow companies to bid on the contract if they are CMMC-certified.

In anticipation of the final CMMC rule, DIBCAC the DoD's ultimate authority on compliance—has increased its audit staff size in response to the pressing need to improve security in the Defense Industrial Base.

How long does it take to get CMMC certified?

Since CMMC Compliance is such a long process, the earlier the company begins, the greater advantage it will have before it becomes law. Obtaining CMMC certification is a comprehensive process that hinges on:

1. An organization's current cybersecurity maturity,
2. The targeted CMMC level, and
3. The schedule of C3PAOs conducting the assessments.

Based on our NIST 800-171 and CMMC compliance preparatory services, below is a general timeframe to become assessment-ready that OSCs need to be aware of:

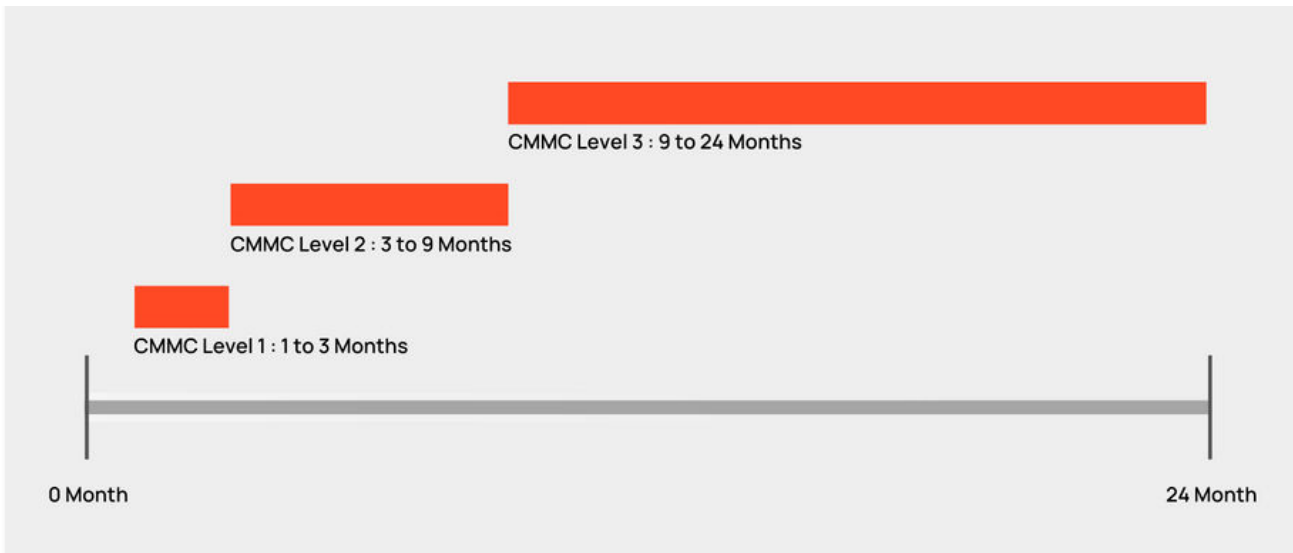


Exhibit 11: CMMC Compliance-Start to Finish Timeline

The following provides a general breakdown of the different stages and their anticipated timelines:

Phase	Duration	Tasks
Self-Assessment and Gap Analysis	1-2 months	Grasping CMMC requirements and examining existing cybersecurity Measures. Identifying and planning to fill compliance gaps.
Implementation	3-18 months	Implementing controls and processes identified in the gap analysis. Adjusting timeframe if major changes are necessary.
Pre-Assessment	1-3 months	Conducting a pre-assessment to ensure preparedness for the official evaluation. Resolving issues identified at this stage.
Official Assessment	1-3 months	Facilitating the official assessment through a C3PAO. Adjusting duration based on the organization's complexity and CMMC level aimed for,
Certification	1-3 months	Receiving certification post successful assessment. Accounting for potential administrative delays.

Exhibit 12: Estimated timeline from start to finish

These timelines are estimations and can vary depending on individual circumstances.

Considering the lengthy nature of this process, it is recommended to initiate preparations as soon as possible and stay updated with the latest guidance from the DoD and the Cyber-AB.

Leveraging the impending enforcement of CMMC, organizations must urgently engage in this process not only to comply with regulatory norms but also to enhance their chances of securing contracts and fostering robust cybersecurity grounded in NIST SP 800-171 and CMMC protocols.

The endeavor will address the critically low implementation rates of NIST SP 800-171, positioning companies more favorably in the competitive landscape once CMMC compliance becomes a legal requirement.

What does the journey to CMMC certification look like?

The journey to CMMC certification is a long one. The company usually begins by identifying where to begin and what level they want to achieve. Your company can begin the journey to CMMC certification by familiarizing itself with the CMMC 2.0 framework. It is important to have background knowledge and know all things CMMC to understand the journey's significance.

Here is what the journey to CMMC Compliance looks like:


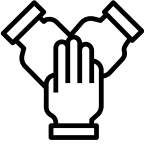

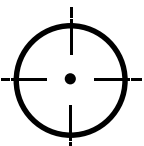


	Ask an Expert	Identifying external partners dedicated to making your company CMMC-certified is important to accelerate your company's process. Registered Provider Organizations (RPOs) can help guide you throughout your journey, saving time and cost.
	Create a CMMC Team	In your organization, forming a team of resourceful experts focused on advancing CMMC progress is vital. These team members should be well-informed and committed to aiding your company in successfully obtaining CMMC certification.
	Identify the Level	When beginning the CMMC journey, you must identify which CMMC level your company wants to achieve. The CMMC level you need to comply with, depends on which contracts and projects your company wants to work on now and in the future.
	Scope the Environment	Once the level is clarified, your organization must scope your compliance boundary. This means there needs to be an in-depth investigation of who deals with CUI or FCI, which devices process it, and what organizational actions are related to it.
	Gap Analysis and Remediation	Your company should conduct a gap analysis to discern its current state and pinpoint existing gaps. If already NIST compliant, your status is advantageous. Following the analysis, remediation will address and resolve identified issues.
	Get Certified!	Level 1 companies perform self-assessment and attestation. Level 2 companies require C3PAO assessment while Level 3 companies require DIBCAC assessment to get CMMC Certification.

Exhibit 13: The CMMC Compliance Journey

What are the challenges faced by small businesses to comply with CMMC?

Small businesses, including those classified as Organization Seeking Certification (OSC) in the defense industrial base, often find themselves grappling with numerous challenges when navigating the path to CMMC compliance.

1. Limited resources

Small and medium-sized businesses (SMBs) and OSCs can find the requirement of significant resources for achieving CMMC compliance a major hurdle largely because the standards of CMMC are grounded in the NIST SP 800-171, which itself is resource-intensive. Such entities often have limited financial provisions, manpower, and technology to comply with these stringent standards fully.

2. Developing CMMC Standard and Unclear Timeline

Since final CMMC enforcement is based on several ifs and buts, it is one of the main causes for the smaller DIBs to stall embarking on the CMMC journey. However, delaying the CMMC Compliance can have detrimental effects on contractors as it may result in lost opportunities.

3. Lack of expertise

Understanding and adhering to the detailed CMMC requirements can be an uphill task due to the limited knowledge and experience in cybersecurity harbored by small enterprises and OSCs. The complexities involved in the foundational standards, including NIST SP 800-171, necessitate deep expertise that these entities often lack.

4. Limited access to information

While the argument that CMMC disproportionately affects OSCs is valid, it doesn't necessarily pertain to the actual requisites of the CMMC program. Small enterprises may, however, need help with procuring detailed information about the standards and the necessary steps toward compliance, making the certification journey an arduous one.

5. Limited access to vendors

A limited pool of credible and approved CMMC readiness vendors or individuals to facilitate businesses in their compliance journey is another significant challenge. The journey toward CMMC certification demands guidance and assistance from seasoned vendors, which is often beyond reach for these businesses. The recent changes in CMMC rule-making have also increased the number of compliance vendors, but 'are they really qualified and have a deep understanding to make CMMC Compliance journey smooth and successful' is the question OSCs need to ask.

6. Limited budget

Financial constraints often limit small businesses' budgets for CMMC compliance. Meeting the stringent CMMC standards usually requires investments beyond OSCs' reach, exacerbating the uneven impact of CMMC on these entities.

What are the CMMC 2.0 assessment requirements?

CMMC Level 1 (Foundational): This Foundational level focuses on the protection of Federal Contract Information (FCI). Level 1 companies are required to self-assess and attest annually.

CMMC Level 2 (Advanced): This Advanced level focuses on the protection of Controlled Unclassified Information (CUI). Level 2 companies are required to undergo a triennial assessment by a C3PAO.

CMMC Level 3 (Expert): This Expert level focuses on the protection of CUI for DoD's highest priority programs. Level 3 companies are required to do triennial government-led assessments.

The image below shows assessment requirements under CMMC 2.0

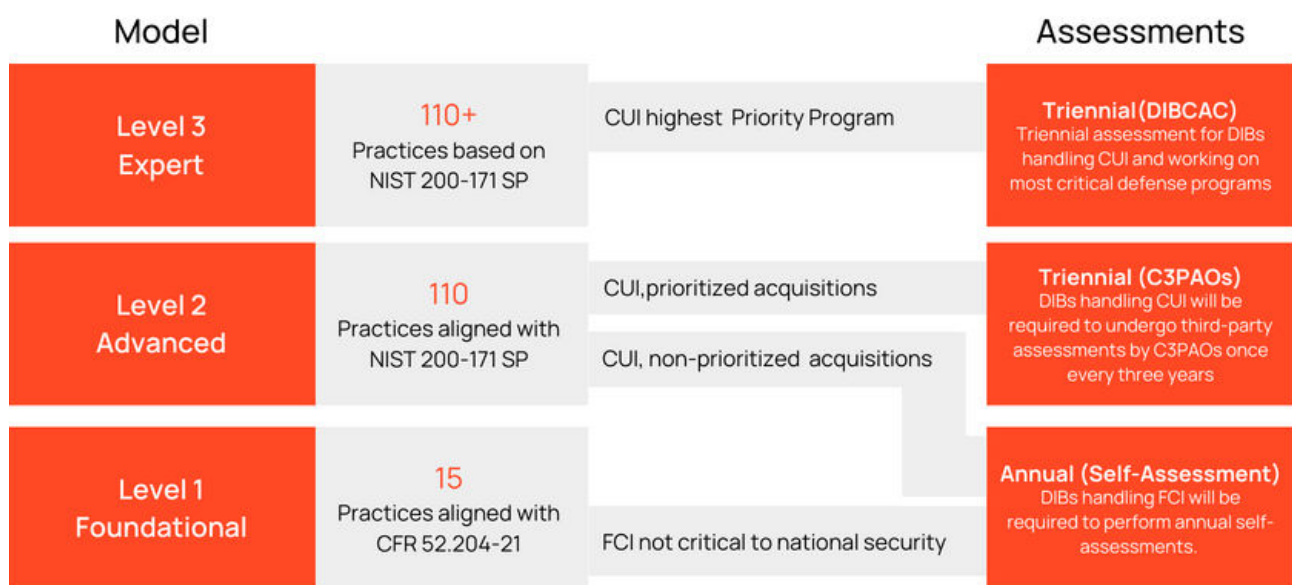


Exhibit 14: Assessment requirements under CMMC 2.0

How much does CMMC Compliance Cost?

The CMMC assessment costs will depend upon several factors, including which CMMC level your company is achieving and the complexity of the DIB company's unclassified network for the certification boundary.

CMMC assessment expenses are predicted to be lower compared to CMMC 1.0 because the Department of Defense has intended to centralize the requirements at all levels instead of unique practices/processes, allowing organizations achieving Level 1 and some Level 2 programs to proceed with self-assessments instead of third-party assessments and strengthen the third-party evaluations.

DoD will release a new cost estimate associated with the CMMC 2.0 program, which will be published on the Federal Register as part of the rule-making process. It is essential to note that the costs for implementing cybersecurity controls arise from the requirement to comply with and safeguard information, defined in FAR 52.204-21 and DFARS 252.204-7012.

(A) One-Time Costs	(B) Monthly Operational Costs	(C) Yearly Licensing / Subscriptions Costs
1. CMMC Readiness Assessment/Gap Analysis	1. Managed Services for Full Users	1. MS365 E5 Licensing
2. Documentation Prep (SSP, Policies and Procedures, SPRS score)	-M365 Infrastructure Support	2. Azure Subscription for the Azure Infrastructure and Duo Implementation
3. Office 365 Implementation to CMMC L2	-Mobile Device Support	3. Duo Federal
4. Azure Implementation to CMMC L2	-Full Desktop Support	4. Email/Drive encryption license
5. MFA to the Desktop built to CMMC L2	-Full 24 x 7 helpdesk	5. Security Awareness Training
6. Implement Email and Drive encryption	2. Managed Services for Infrastructure	6. Phishing Exercises
7. Managed IT Services	-Firewall Management	
8. Managed Security Services Onboarding	-Server Management	
9. Third Party Assessment (C3PAO)	-Azure Infrastructure Support	
10. Assessment Support	-Microsoft Premier Support	
	-Full 24 x 7 NOC	
	3. Managed Security Services	
	-SIEM Management	
	-Vulnerability Management	
	-Intrusion Detection / Incident Response	
	-Threat Feed Integration	
	-Full 24 x 7 SOC	
Fully Burden Costing (A+B+C)*		
This will range from (low) \$250 to (high) \$7,500 cost per seat, depending on the firm's size and the work's complexity.		

Exhibit 15: Sample Cost Components

Here are the cost considerations to keep in mind for CMMC compliance for your company. Get expert insights on how to minimize these costs to obtain and maintain your CMMC certification.



CMMC Level you want to certify under



The number of people handling CUI Data



Time required to prepare



Existing Security Compliance such as NIST and ISO 27001



Tools and technology solution license and implementation cost



C3PAO assessment cost. MSP or MSSP fee to support assessment



The complexity of the Business

Exhibit 16: Factors affecting the cost of compliance

What are some of the most challenging controls to implement?

Based on our past NIST 800-171 and CMMC compliance engagements with our customers, we observed that the following controls were typically difficult to implement and sustain operationally.

NIST 800-171 Controls	CMMC 2.0 Practices	Control Synopsis
3.1.3	AC.L2-3.1.3	Control the flow of CUI in accordance with approved authorizations.
3.1.7	AC.L2-3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
3.1.9	AC.L2-3.1.9	Provide privacy and security notices consistent with applicable CUI rules.
3.1.11	AC.L2-3.1.11	Terminate (automatically) a user session after a defined condition.
3.1.20	AC.L2-3.1.20	Verify and control/limit connections to and use of external information systems.
3.3.1	AU.L2-3.3.1	Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.
3.3.3	AU.L2-3.3.3	Review and update audited events.
3.3.4	AU.L2-3.3.4	Alert in the event of an audit logging process failure.
3.4.7	CM.L2-3.4.7	Restrict, disable, and prevent the use of nonessential programs, functions, ports, protocols, and services.
3.5.3	IA.L2-3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to nonprivileged accounts.
3.6.3	IR.L2-3.6.3	Test the organizational incident response capability.
3.8.7	MP.L2-3.8.7	Control the use of removable media on system components.
3.13.11	SC.L2-3.13.11	Employs FIPS-validated cryptography when used to protect the confidentiality of CUI.
3.13.13	SC.L2-3.13.13	Control and monitor the use of mobile code.
3.13.16	SC.L2-3.13.16	Protect the confidentiality of CUI at rest.
3.14.1	SI.L2-3.14.1	Identify, report, and correct information and information system flaws in a timely manner.

Exhibit 16: Most challenging controls to implement

What is the difference between Basic, Medium, and High assessments?

Basic Assessment

Contractor self-assessment of system security plan(s), resulting in a "low" confidence level in the resulting score.

Medium and High Assessment

Defense Contract Management Agency's (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) review of the system security plan(s), resulting in a "medium" or "high" level of confidence in the resulting score.

Which controls are consistently failing DIBCAC assessments?

Around November of 2022, DIBCAC Director for the Defense Contract Management Agency (DCMA), Nick DeI Rosso, provided insights into the Top 10 controls often determined to be Other Than Satisfied (OTS) during DIBCAC assessments of DIB organizations.

NIST 800-171 Controls	CMMC 2.0 Practices	Practice Statement
3.5.3	IA.L2-3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to nonprivileged accounts.
3.13.11	SC.L2-3.13.11	Employs FIPS-validated cryptography when used to protect the confidentiality of CUI.
3.14.1	SI.L1-3.14.1	Identify, report, and correct information and information system flaws in a timely manner.
3.11.1	RA.L2-3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.
3.11.2	RA.L2-3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.
3.3.3	AU.L2-3.3.3	Review and update logged events.
3.3.4	AU.L2-3.3.4	Alert in the event of an audit logging process failure.
3.3.5	AU.L2-3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.
3.6.3	IR.L2-3.6.3	Test the organizational incident response capability.
3.4.1	CM.L2-3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.

Exhibit 17: Controls consistently failing DIBCAC assessments

What is SPRS?

The DoDI 5000.79 "Defense-Wide Sharing of Supplier Performance Information (PI)," published on October 15, 2019, established policy and assigned responsibilities for managing the defense-wide collection and sharing of performance information on suppliers, products, and services.

[DoD Supplier Performance Risk System \(SPRS\)](#) is a procurement risk analysis tool for Price, Item, and Supplier risk. The Price Risk tool compares industry prices to the average price paid by the government. The Item Risk tool flags items identified as high risk (based on critical safety/application or risk of counterfeiting). The Supplier Risk tool scores vendors on DoD-wide contract performance.

SPRS supports DoD Acquisition Professionals with meeting acquisition regulatory and policy requirements by providing the following:

- On-time delivery scores and quality classifications (DFARS 213.106-2)
- Price, Item, and Supplier procurement risk data and assessments
- Company exclusion status (debarments, suspensions, etc.)
- NIST SP 800-171 Assessment results
- National Security System Restricted List
- Supply chain illumination

SPRS provides storage and access to the NIST SP 800-171 assessment scoring information. The NIST SP 800-171 Assessments module contains the assessment date, score, scope, and plan of the action completion date, Included Commercial and Government Entity (CAGE) code(s), System Security Plan (SSP) name, SSP version, SSP date, and confidence level.

The NIST SP 800-171 Basic Assessment cannot be performed in SPRS; SPRS only stores the results of NIST SP 800-171 Assessments.

An "SPRS Cyber Vendor User" role is required for companies to enter/edit basic self-assessment information. One may be created if a record header for the Highest-Level Owner (HLO) does not exist. Once the HLO header has been created, assessments for CAGEs who fall within the HLO hierarchy may be added.

All DIBs, regardless of CMMC 2.0 Level, must upload their SPRS score, SSP, and POA&Ms into the DoD SPRS system.

Are POA&Ms allowed in CMMC 2.0?

The Department of Defense (DoD) will permit the use of POA&Ms (Plan of Action and Milestones) for companies who have not yet met all the security controls at the time of award of defense contracts under CMMC 2.0. However, POA&Ms will not be allowed for the most critical security requirements, which are the most difficult to meet.

The DoD uses a self-assessment method that assigns a weight of 1, 3, or 5 points to each of the 110 controls in NIST SP 800-171. The scoring starts at a maximum of 110, and points are subtracted for each control not yet implemented. As most controls are worth more than one point, the self-assessment scores can be negative and range from -203 to +110.

Although final information has not yet been released, Stacy Bostjanick, the director of the CMMC program for the DoD, stated in June 2022 that POA&Ms will be allowed for controls weighted at 1 or 3 points but not for controls weighted at 5 points.

The DoD also plans to set a minimum score that must be achieved when using POA&Ms for CMMC certification, and POA&Ms will have a time limit, which will be strictly enforced. The time limit has not been decided yet, but it is considered 180 days. It is also not yet known when the 180-day POA&M clock will start, but it is likely to be upon the award of a contract, either by DoD to a prime contractor or by a contractor to a subcontractor.

Are waivers allowed in CMMC 2.0?

To maintain flexibility and the ability to act quickly, the Department of Defense (DoD) will allow for limited waivers in the CMMC 2.0 program. These waivers will only be granted for certain mission-critical contracts and require a detailed justification package, including a plan for risk mitigation and a timeline for meeting CMMC requirements. Approval for waivers will come from high-level DoD leadership and apply to the entire CMMC requirement, not just individual controls. More information on waivers will be established during the rulemaking process.

Will prime contractors and subcontractors be required to maintain the same CMMC level?

If contractors and subcontractors are handling the same type of FCI and CUI, then the same CMMC level will apply. In cases where the prime only flows down select information, a lower CMMC level may apply to the subcontractor.

Will my organization need to be certified if it does not handle CUI?

If a DIB company does not process, store, or transmit CUI on its unclassified network, but does process, store or handle 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.

Who oversees CMMC within a company: the FSO or the IT director?

The responsibility for CMMC management falls under whoever oversees cybersecurity in your organization, which encompasses personnel, facilities, and technology. It can vary based on your company's structure and the roles defined by its leadership.











Will my assessment outcomes be accessible to the public and the DoD?

The DoD will have access to your assessment details including results and the final report once CMMC 2.0 is fully operational, storing this data in the SPRS and eMASS databases. However, it is not specified if the results will be publicly available.

How should a company handle situations where complete CMMC implementation interferes with necessary system functionality?

CMMC assessments aim to ensure systems handling DoD CUI meet the security requirements outlined in specific FAR and DFARS clauses, including adhering to the "adequate security" standard of NIST SP 800-171. If full CMMC deployment compromises system functionality, the concerned system should not be used to process, store, or transmit DoD CUI, as it fails to satisfy the necessary security prerequisites to safeguard such information.

What are the 17 CMMC Domains?

	Domain Name	Domain Description
	Access Control	Requires your organization to establish who has access to your systems and what their requirements are to operate effectively. As well who has remote access, internal system access, and the limitations of their roles in system.
	Asset Management	This domain asks that you locate, identify, and log inventory of the assets to your organization.
	Audit & Accountability	Requires a system to track and audit users accessing your organization's CUI, ensuring accountability through defined audit requirements, secure results protection, and audit log management.
	Awareness & Training	This domain requires that you have training programs in place for all personnel and conduct security awareness activities.
	Configuration Management	This domain asks that you establish configuration baselines as a measure to judge the efficiency of your systems. This is necessary to conduct audits and accurately measure the posture of your systems.
	Identification & Authentication	This domain ensures the proper roles within your organization have the correct level of access and can be authenticated for reporting and accountability purposes.
	Incident Response	For this domain, your organization needs an Incident Response Plan to detect and report events, respond to incidents, conduct post-incident analyses, and test readiness for cyber attacks.
	Maintenance	This domain requires you have a maintenance system in place to maintain and effectively operate your systems.
	Media Protection	In this domain, your organization must demonstrate that it has properly labeled media for easy access, and showcases media protection, sanitation, and transportation security protocols.
	Personnel Security	Your personnel will have to have been properly screened and have background checks run. Also, you will need to provide evidence that your CUI is protected during personnel activity such as employee turnover or transfer.


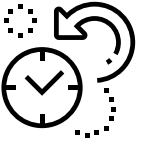



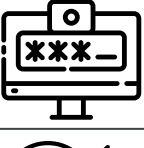
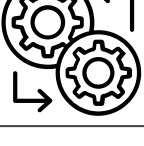
	Physical Protection	Your organization will need to provide evidence of the physical security surrounding your assets and prove that they are protected.
	Recovery	This domain requires that you keep and log backups of media necessary to your organization, these need to be logged for the purpose of continuity among backups and mitigate lost data.
	Risk Management	Risk Management is the process of identifying and evaluating the risk that affects your company using periodic risk assessments and vulnerability scanning. This includes your own organization's risk as well as that of your vendors.
	Security Assessment	For this domain, you will need a system security plan in place. Additionally, you will need to define and manage controls and perform code reviews for your organization.
	Situational Awareness	You will need evidence of a threat monitoring system. This helps supplement other domains and keeps your organization secure in the event of a cyber incident.
	System & Communication Protection	You will need to define the security requirements of each system and communication channel your organization uses to provide evidence your organization has control of communications at system boundaries.
	System & Information integrity	System and information integrity require you to identify and manage flaws within your system, identify hazardous and malicious content in-system, implement email protections and monitor your network and system.

Exhibit 18: List of 17 CMMC Domains?

How can an RPO help in CMMC Compliance?

Achieving compliance with the Cybersecurity Maturity Model Certification (CMMC) can be challenging for DIB Contractors. However, by working with a Registered Provider Organization (RPO), contractors can gain access to the guidance, expertise, and resources necessary to successfully navigate the requirements and best practices for each maturity level. Here are a few of the benefits of working with Intersec:

- **Hundreds of DFARS assessments and readiness experience.**
- **A rigorous CMMI Services Level 3** mature service delivery process and ISO 9001 quality management to the CMMC services.
- **CyberAB Registered Provider Organization (RPO)** with many seasoned cybersecurity solutions architects, Registered practitioners, CMMC CCPs, and CCAs.
- Prime contractor on the Virginia GENEDGE CMMC services BPA and a **vetted CMMC compliance service provider.**
- **Expert in CMMC Policy Procedures and Technical Remediation.**
- **Simplified technical implementation** with significantly less operational cost.
- Recommendations for some technical controls that don't cost a thing.
- Easy to **customizable services and price models** to fit very small to mid-size organizations.
- **Rapid CUI scoping** to right-size your CMMC compliance efforts.
- Our experts, tools, and accelerators mean **30% quicker compliance readiness**, saving time and money for our customers.
- **MSSP services** for ongoing CMMC compliance.

Partnering with an RPO like InterSec can **significantly increase a DIB Contractor's chances of quickly achieving and maintaining CMMC compliance.** InterSec, a Cyber-AB RPO, has years of experience helping Federal Contractors navigate complex compliance requirements. As a Cybersecurity organization, we provide end-to-end CMMC Compliance consulting.

We provide a compliance-accelerated platform and rapid CUI scoping to begin your CMMC compliance journey. We have expertise in technical remediation and provide audits for your company. We are a dedicated team of professionals to help your company meet your CMMC needs through cost-effective solutions. Our bespoke solutions and services save your company valuable time, resources, and money in achieving CMMC compliance.

As a Cyber-AB authorized CMMC RPO, Intersec offers Consulting, Gap Assessment, Remediation, and Managed Security Services to ramp up and accelerate your CMMC Compliance Journey.



[Schedule a 30 min complimentary CMMC Consultation](#)



[Send an email for requesting free CMMC Consultation](#)

Case Study 1 : Unleashing CMMC Success

How InterSec helps a manufacturing company meet CMMC requirements with ease.

Introduction

A Virginia-based manufacturing company was facing challenges in meeting the Cybersecurity Maturity Model Certification (CMMC) Level 2 requirements set forth by the Department of Defense. The company had limited IT resources and was hesitant about using cloud services.

Problem

The company was struggling to meet the CMMC requirements due to its limited IT resources, lack of dedicated IT staff, and use of outdated technology. Additionally, the company was cautious about using cloud services to store sensitive information.

Solution

InterSec was referred to the company to help them achieve CMMC compliance. InterSec engaged the company's executive management, educated the company's staff, and defined roles and responsibilities for information security. InterSec then utilized its NIST 800-171/CMMC field-tested readiness methodology to ensure a successful CMMC compliance milestone.

Methodology

- Controlled Unclassified Information (CUI) scoping
 - Gap analysis
 - A current state analysis of the client's organization security
 - Development of a remediation plan
 - Policies and procedures development
 - Technical remediation services, including asset management, multi-factor authentication, vulnerability scanning, email encryption, drive encryption, and virtual private network
-

Results

InterSec was able to quickly remediate and improve the company's security posture, resulting in an SPRS score of 110. The client subsequently requested our Managed Security Service Provider (MSSP) services to maintain CMMC compliance.

Conclusion

InterSec's well-defined methodology, streamlined project execution, and expertise made the project a success, helping the company achieve the CMMC requirements and secure its systems. The company can now continue serving the defense industry while minimizing potential security risks.

Case Study 2 : Accelerating CMMC compliance

A Virginia-based acquisition support contractor's success story with InterSec

Introduction

A Virginia-based Acquisition Support contractor with 200+ employees was facing challenges in meeting the Cybersecurity Maturity Model Certification (CMMC) Level 2 requirements set forth by the Department of Defense. With two office locations and a recent acquisition of a small manufacturing company, the contractor needed to comply with a defense contract and improve the SPRS score to 110.

Problem

The contractor faced the complex task of integrating the acquired company employees into its existing systems, and employees were not on the parent company's Active Directory which made it harder to enforce CMMC policies and procedures.

Solution

InterSec came to the rescue with its innovative approach to CMMC compliance, leveraging its CMMC accelerators and field-tested NIST 800-171/CMMC methodology to assess the current state and develop a remediation plan. The plan was executed by creating policies, and procedures, supplement documents, and providing technical remediation services.

Methodology

InterSec brought a rigorous CMMI Services Level 3 mature service delivery process and ISO 9001 quality management to CMMC services, conducted an assessment, developed a remediation plan, implemented policies/procedures, provided technical remediation services, integrated the acquired company, prepared documentation, and executed the project using their NIST 800-171/CMMC field-tested readiness methodology, resulting in a successful outcome for the customer.

Results

The contractor's SPRS score improved to 110, the acquisition was seamlessly integrated into the parent company's systems, and all required documentation was uploaded into the SPRS system ahead of the deadline, meeting the customer's CMMC compliance requirements.

Conclusion

InterSec's innovative approach and experienced team helped the contractor achieve CMMC compliance and secure their systems, ensuring their ability to serve the defense industry while minimizing security risks. The well-defined methodology and field-tested approach to execution made the project a resounding success.

Appendix

CMMC Glossaries

TERM	DEFINITION
Asset Owner	A person or group with primary responsibility for the viability, productivity, security, and resilience of an organizational asset.
Cybersecurity Maturity Model Certification (CMMC)	The set of requirements the Department of Defense has which an organization seeking certification (OSC) is assessed by. A certification process is now required for businesses seeking contracts with the DoD.
CMMC Assessment	The formal process of assessing the implementation and reliable use of controls through interviews, document reviews, and other observation measures. For CMMC specifically, an assessment is performed by an organization AND on an organization to see if they meet the requirements for the CMMC Level they are achieving certification for.
CMMC Audit	Performed by a C3PAO or CA and sanctioned by Cyber-AB, this is the process where an official professional or organization will check your organization against a given level of CMMC that you are achieving certification for to see if you successfully meet the requirements for that level. If you pass the audit, you're issued the certification for that CMMC level.
CMMC Certified Assessor (CA)	A cybersecurity professional who has completed the background, training, and examination requirements to be certified at one of three levels by Cyber-AB. They are the ones who usually perform an audit on an organization.
CMMC Certified Professional (CP)	An individual authorized to participate as an assessment team member under the supervision of a Certified Assessor and authorized to have CMMC training.
CMMC Certified 3rd Party Assessment Organization (C3PAO)	An organization that has been certified by Cyber-AB to be contacted to provide consulting or certified assessments for an organization seeking certification for CMMC at any given level.
CMMC Certified Organization	An organization that has passed a CMMC Audit successfully and been issued a CMMC Certificate for a given level by the Cyber-AB.
CMMC Control	The policies and procedures to protect the organization's assets, maintain efficiency and stay within established standards. For CMMC, there are a total of 110+ controls that need to be met for full Level 3 certification, though Level 1 starts out with only 17.
CMMC Domain	Part of the CMMC model framework, domains are the categories of the framework, which are further broken down into a set of processes and practices with different topics related to the security of an organization. There are 17 domains within CMMC.
CMMC Maturity Level	This term is used to describe the security practices of a Defense Contractor found eligible for a CMMC-assessed seal after going through an audit sanctioned by the Cyber-AB. There are 3 maturity levels: Level 1: Foundational, Level 2: Advanced, and Level 3: Expert.

TERM	DEFINITION
CMMC Registered Provider Organization (RPO)	A company authorized to represent itself as familiar with the CMMC Standard (given a Cyber-AB standardized logo) and is able to deliver CMMC consulting to organizations seeking certification (non-certified consulting). InterSec is a CMMC Registered Provider Organization.
CMMC Registered Practitioner (RP)	An individual who has gone through training to provide consulting services or advice related to CMMC to an OSC that is non-certified. They do not participate in official audits.
Controlled Unclassified Information (CUI)	Sensitive information that requires safeguarding and is protected with the aid of law, regulations, and government-wide policies.
Department of Defense (DoD)	Executive department of the United States federal government. It is responsible for the nation's military affairs, including research, development, and procurement. It also directs operations by the armed forces. The DoD is the agency responsible for creating the CMMC model.
Defense Contractor	Organizations (generally privately owned) that provide products and services to the Department of Defense. They must have at least one contract with the DoD to do so.
Defense Industrial Base (DIB)	The industrial complex is the worldwide network of companies, universities, and institutions that create, produce, or otherwise supply weapons, computers, and other products used by the US military. Most Defense Contractors are considered a part of the DIB.
Dispute Adjudicator	An employee from Cyber-AB who is responsible for handling disputes between an Assessor and OSC for an Assessment/Audit.
Federal Contract Information (FCI)	Proprietary information (not intended for public release) that is generated under contract to develop or deliver a product or service to the Government.
Gap Analysis	A gap analysis is a tool that companies can use to compare their current performance with how they strive to perform. For CMMC, it is usually a report that identifies where an organization lacks security regulations, implementations, and requirements (similar to a POA&M).
NIST SP 800-171	A standard published by the National Institute of Standards and Technology (NIST). The 113-page document outlines the security requirements organizations must satisfy to protect CUI data in non-federal systems. The document lists 110 requirements (or controls) that makeup CMMC levels 1-2.
Organization Seeking Certification (OSC)	An organization that intends to go through the CMMC assessment process and become certified under CMMC for a particular level.
Plan of Action and Milestones (POA&M)	A document that identifies missing security requirements and objectives and provides a timeline for their resolution. Cybersecurity professionals produce this document.
System Security Plan (SSP)	An SSP is a document describing an organization's information security policies, practices, and procedures. This is required at CMMC Level 2 and beyond and is an important document used in the audit process.

FREE CUI WHITEPAPER

Federal agencies and their external service providers routinely generate, use, store, and share information that, while not meeting the standards for classified national security information nevertheless requires safeguarding and dissemination controls.

We have created a whitepaper that discusses Controlled Unclassified Information (CUI) and how to protect it best. This Whitepaper covers:

- US Government's document handling restrictions and control mechanism to safeguard protected unclassified information.
- Guidance on identifying, using, storing, and sharing CUI.



INDEX OF CUI WHITEPAPER

1. What is CUI?
2. Why is the CUI Program Necessary?
3. Identifying CUI
4. CUI lifecycle
5. Who can view CUI?
6. Types of CUI
7. Other Categories
8. CUI Marking Guidance
9. Protection Barriers
10. Access and Information Systems Controls
11. Disposing CUI
12. What is CMMC?



[CLICK HERE TO DOWNLOAD THE FREE CUI WHITEPAPER](#)







FOR MORE INFORMATION

DOD CUI Program Website: <https://www.dodcui.mil/>

DOD CUI Registry: <https://www.dodcui.mil/Home/DoD-CUI-Registry/>

DOD Mandatory Controlled Unclassified Information Training (for DOD and Industry):
<https://securityawareness.usalearning.gov/cui/index.html>

Why do DIBs choose InterSec as a CMMC Compliance partner?

-  InterSec brings a rigorous CMMI Services Level 3 mature service delivery process and ISO 9001 quality management to the CMMC services.
-  InterSec is a Cyber-AB RPO with many seasoned RPs and assessors.
-  A prime contractor on the Virginia GENEDGE CMMC services BPA, so you can count on us as a vetted CMMC compliance service provider.
-  A dedicated team of security professionals is available to you throughout the CMMC compliance process.
-  Strategic partnerships and alliances with product vendors to provide turnkey and cost-effective solutions to meet CMMC compliance.
-  Multiple services and price models that can be easily customized to meet your organization's unique needs.

OUR APPROACH TO CMMC COMPLIANCE

At InterSec, we take CMMC compliance seriously, and we have developed an approach that ensures our clients are fully prepared for compliance. Our approach involves assessment, remediation, and ongoing monitoring to ensure guaranteed compliance:

ASSESS CMMC GAP ASSESSMENT	DEFEND REMEDIATION	SECURE ONGOING MONITORING
<ul style="list-style-type: none"> • SCOPING TO EVALUATE APPLICABLE CMMC LEVEL • IDENTIFY CUIS, FCIS • ESTABLISHING EXISTING CYBERSECURITY MATURITY • ASSESS COMPLIANCE • SPRS EVALUATION • POA&MS WITH ACTIONABLE REMEDIATION GUIDANCE 	<ul style="list-style-type: none"> • DOCUMENTATION AND TECHNICAL REMEDIATION • ESTABLISHING EXISTING CYBERSECURITY MATURITY • ASSESS COMPLIANCE • SPRS SCORE • POA&M • SYSTEM SECURITY PLAN • ACTIONABLE REMEDIATION REPORT 	<ul style="list-style-type: none"> • PERIODIC POLICIES AND PROCEDURES REVIEWS AND UPDATES • INCIDENT RESPONSE TABLE TOP EXERCISE • ANNUAL PHISHING EXERCISES • SECURITY AWARENESS TRAINING • PERIODIC VULNERABILITY SCAN • SPRS SCORE UPDATES



Rapid CUI scoping to right-size your CMMC compliance efforts



Discounted CMMC Level 2 Gap Assessment



Expertise in CMMC Technical Remediation



CMMC audit-ready artifacts for quick turnaround



CMMC Pre-audit to baseline the existing cybersecurity readiness



MSSP services for ongoing CMMC compliance



Hundreds of DFARS assessments and readiness experience

170+

NIST 800-171 SSP, POA&M, AND SPRS

200+

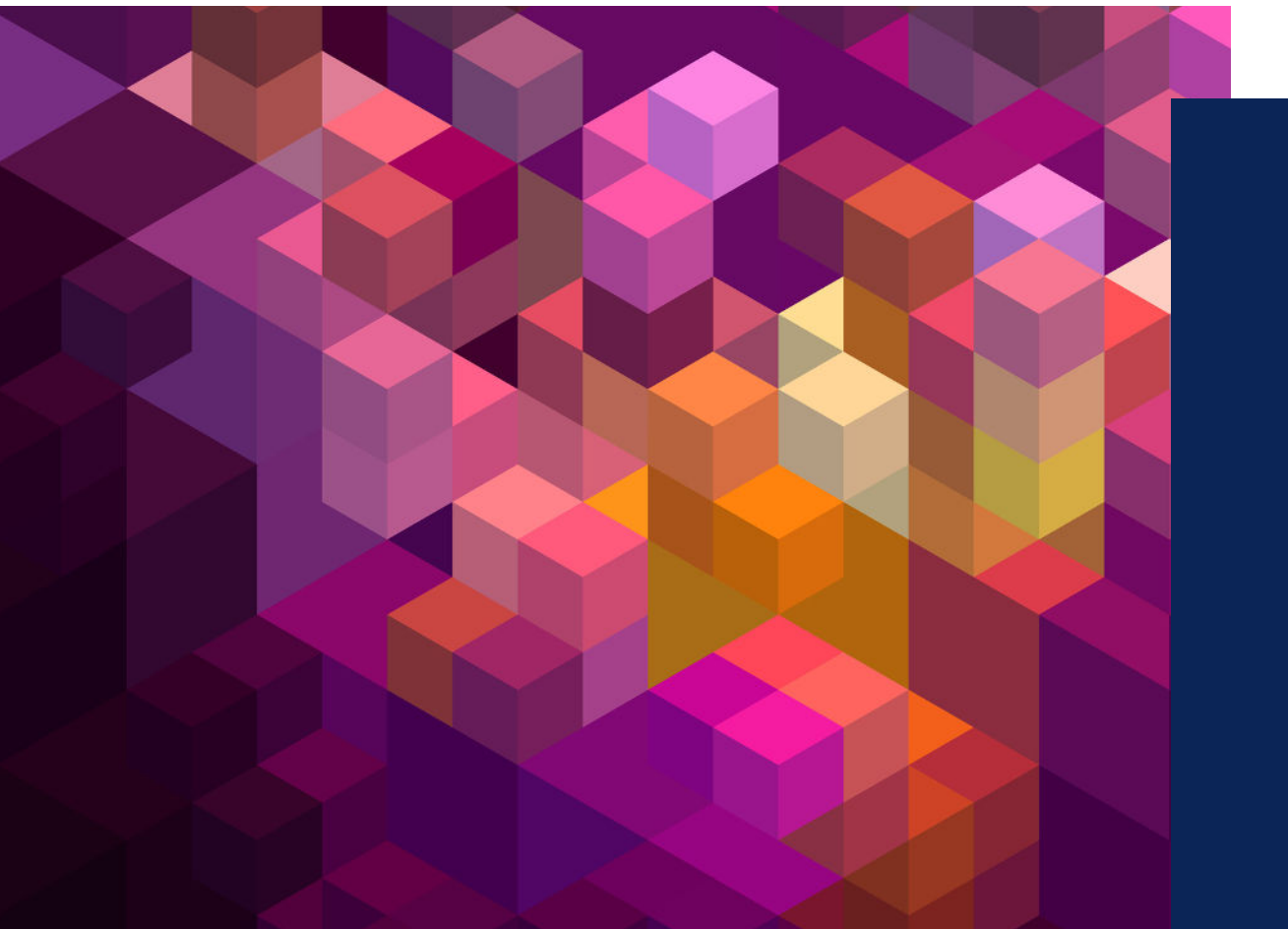
LEVEL 1 ADVISORY AND CONSULTING

50+

LEVEL 2 ADVISORY, CONSULTING, AND MSSP

OUR CLIENTS





Ready to start your CMMC Journey?

Please contact us at complianceservices@intersecinc.com

Call us at [\(833\) 228-4858](tel:8332284858) (toll-free)

Website: www.intersecinc.com

NAICS Codes: 541511, 541512, 541519

GSA Multiple Award Schedule Contract: 47QTCA19D00EG

54151S – Information Technology (IT) Professional Services,

54151HACS – Highly Adaptive Cybersecurity Services (HACS), and OLM – Order Level Materials.