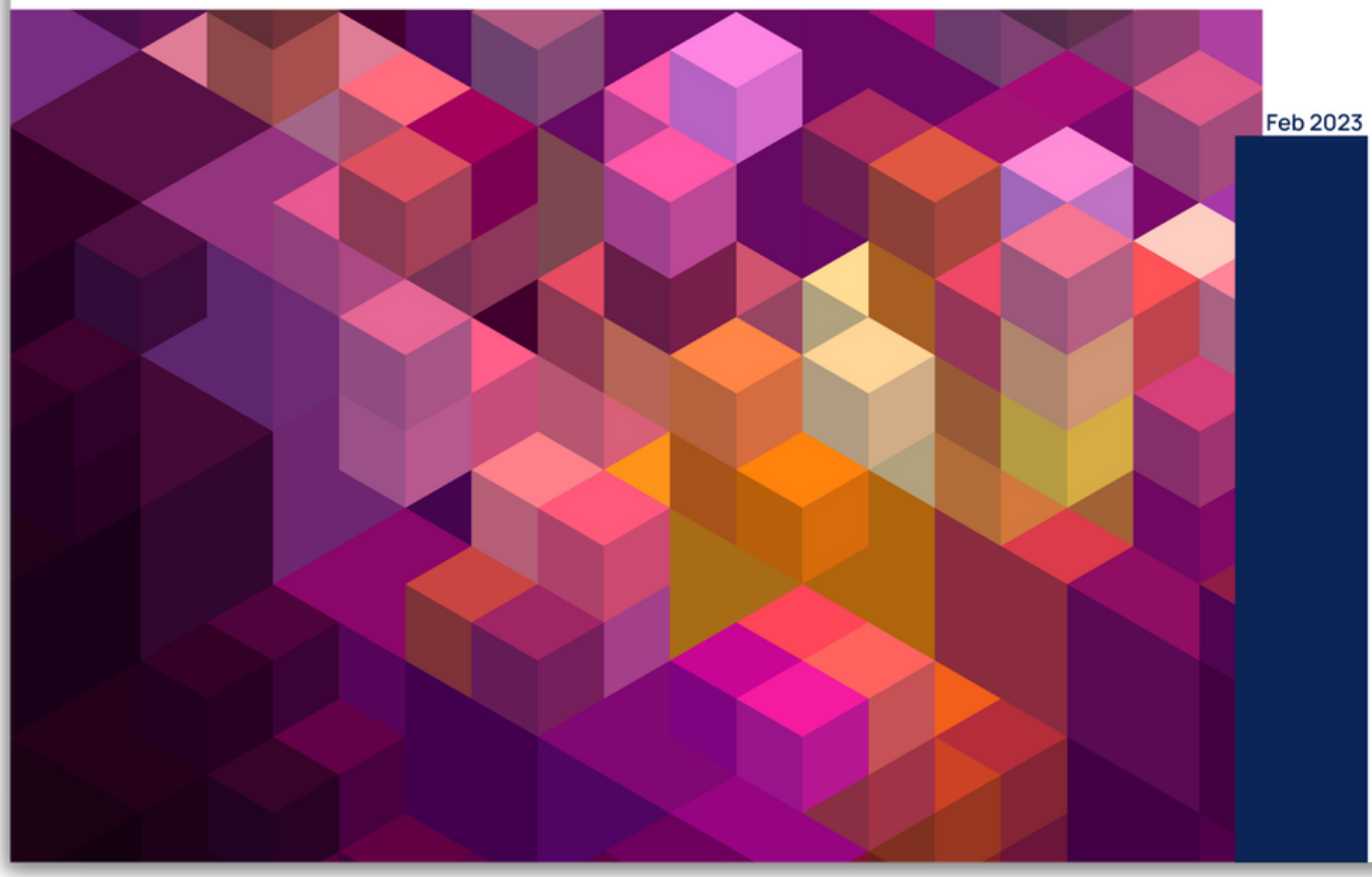
InterSec
Ignite . Inspire. Innovate

CMMI SVC /3

CYBERSECURITY MATURITY MODEL CERTIFICATION

A FEDERAL CONTRACTOR'S GUIDE TO CMMC 2.0



InterSec
Ignite . Inspire. Innovate

CYBERSECURITY MATURITY MODEL CERTIFICATION

A FEDERAL CONTRACTOR'S GUIDE TO CMMC 2.0

Mar 2023

Synopsis

Welcome to our most comprehensive guide on CMMC 2.0!

The Cybersecurity Maturity Model Certification (CMMC) is a program implemented by the U.S. Department of Defense (DoD) to ensure that organizations handling controlled unclassified information (CUI) have appropriate cybersecurity controls in place to protect sensitive information from unauthorized access, use, or disclosure.

CMMC 2.0 introduces a tiered system of levels, ranging from Level 1 (Basic Cybersecurity Hygiene) to Level 3 (Advanced/Progressive).

But why is CMMC compliance important? As cyber threats evolve and become more sophisticated, organizations must prioritize cybersecurity to protect their assets and data. CMMC compliance will soon be a requirement for DoD contractors, with requirements appearing in solicitations starting by Fall 2023.

If your organization handles CUI for the DoD, it is important to understand which CMMC level you need and begin the journey toward certification.

There are many benefits to achieving CMMC compliance, including increased credibility and competitiveness in the market, improved cybersecurity posture, and protection of sensitive information.

However, small businesses may face challenges in complying with CMMC, including limited resources and a lack of understanding of the process.

The journey toward CMMC certification can take anywhere from a month to 2 years, depending on your organization's complexity, locations, current cybersecurity posture, and the level of certification you are seeking.

The cost of CMMC compliance can vary, but it is important to carefully consider your budget and work with a professional consulting firm to find a solution that fits your needs.

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

Index

1. BACKGROUND AND CONTEXT

- What is NIST 800-171?
- Why did NIST 800-171 fall short?
- How did CMMC evolve?

2. CMMC 2.0 FRAMEWORK

- Key Changes to CMMC 2.0
- What are the CMMC 2.0 Levels?
- How many domains and practices does CMMC 2.0 have?
- Why is CMMC compliance important?

3. THE CMMC ECOSYSTEM

- Who does CMMC apply to?

4. CMMC: FROM READINESS TO CERTIFICATION

- How long does it take to get CMMC certified?
- When will CMMC requirements start appearing in solicitations?
- What CMMC level do I need?
- What does the journey to CMMC certification look like?
- What are the challenges faced by small businesses to comply with CMMC?
- What are the CMMC 2.0 assessment requirements?
- What are some of the most challenging controls to implement?
- Which controls are consistently failing DIBCAC assessments?
- What is the difference between Basic, Medium, and High assessments?
- What is an SPRS?
- Are POA&Ms allowed in CMMC 2.0?
- Are waivers allowed in CMMC 2.0?
- How much does CMMC Compliance Cost?

5. HOW CAN AN RPO LIKE INTERSEC HELP IN CMMC COMPLIANCE?

- Case Study 1 : Unleashing cybersecurity success
- Case Study 2 : Accelerating CMMC compliance

Background and Context of CMMC

What is NIST 800-171?

The Department of Defense (DoD) mandated in 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-assessments.

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 does not address the strength and maturity utilized to fulfill the requirement.

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

© INTERSEC, INC. ALL RIGHTS RESERVED

How did CMMC evolve?

2015-2020

In 2015, the National Institute of Standards and Technology (NIST) released Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

Subsequently, the Department of Defense (DoD) issued contract clause 252.204-7012 to enforce compliance by the Defense Industrial Base (DIB) with the NIST 800-171 control requirements. The DIB was required to self-attest their compliance with NIST SP 800-171's 110 controls by late 2017.

Despite the implementation of regulations aimed at preventing it, the continued occurrence of CUI (Confidential Unclassified Information) breaches remains a threat to national security in the United States.

This regulation was insufficient because NIST 800-171 relied on self-assessments. This was problematic because of the complexity of cybersecurity controls, improper implementation, and subjective self-assessment, and in some cases, some companies just checked the box without knowing anything about the compliance requirement. The lack of rigor in the enforcement of NIST 800-171 compliance caused the DIB to continue to be vulnerable to cyber threats including APTs (Advanced Persistent Threats).

In 2020, the DoD released its Cybersecurity Maturity Model Certification (CMMC) 1.1 framework that mandated in early 2020 that all organizations exchanging CUI implement the 110 security controls listed in NIST SP 800-171 to safeguard the CUI.

CMMC addresses requirements for the protection of FCI and CUI data:

1. 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.

2. 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.

© INTERSEC, INC. ALL RIGHTS RESERVED

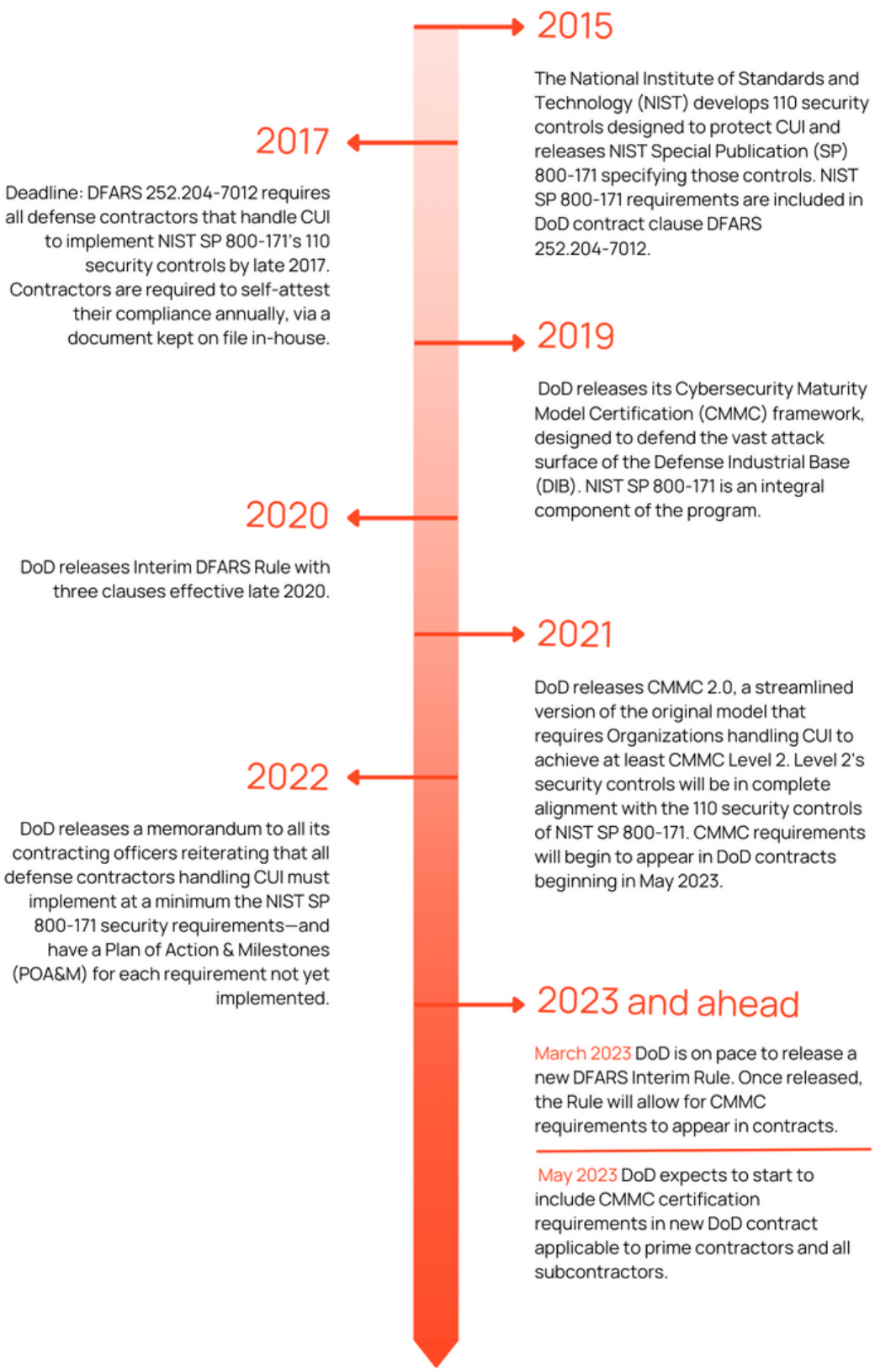


Exhibit 1 : The CMMC Evolution Timeline

© INTERSEC, INC. ALL RIGHTS RESERVED

2021-Present

The CMMC program's original form was criticized for its complexity and anticipated certification costs. Driven by feedback across the industry, CMMC has since been reworked into a hybrid certification model. This new version, referred to as CMMC 2.0, was announced on November 4, 2021.

The changes are intended to reduce barriers to compliance for small and mid-sized firms while maintaining the goal of protecting the Defense Industrial Base from cyber-attacks. CMMC 2.0 focuses on the most critical requirements and streamlines the model from 5 to 3 compliance levels.

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 covered 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 Nonfederal Information Systems and Organizations" in effect at the time the solicitation is issued or as authorized by the contracting officer.**

More to come on CMMC

In March, 2023, DoD is on pace to release a new DFARS Interim Rule that will codify CMMC into law via the DFARS 7021 clause. Once released, the Rule will allow CMMC requirements to appear in contracts.

In May, 2023, DoD expects to include CMMC certification requirements in new DoD contracts. CMMC requirements will apply to prime contractors and all subcontractors throughout their supply chain.

© INTERSEC, INC. ALL RIGHTS RESERVED

CMMC 2.0 Framework

> CMMC was created to defend the defense industrial base (DIB) from increasingly frequent and sophisticated cyberattacks. It 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 has replaced the five cybersecurity compliance levels in CMMC 1.0.

Key Changes to CMMC 2.0

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.

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

Exhibit 2 : Simplified CMMC 2.0

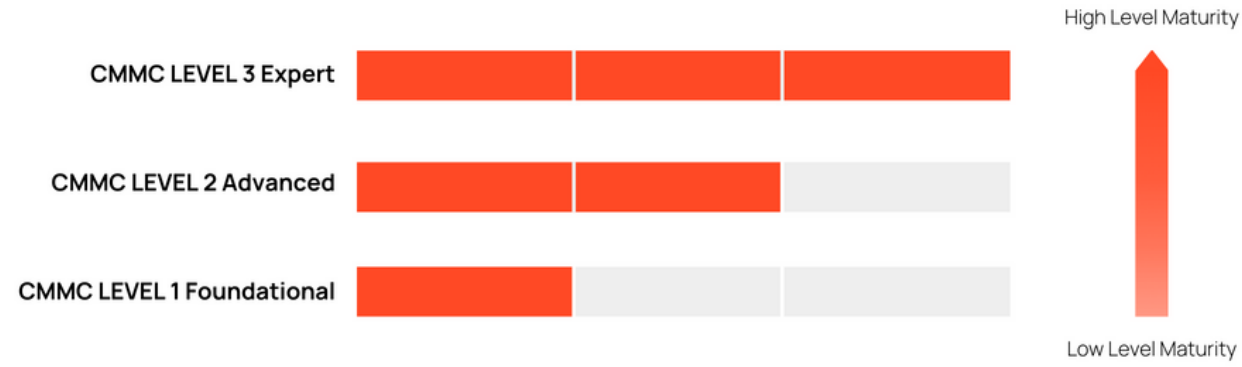
© INTERSEC, INC. ALL RIGHTS RESERVED

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 includes 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.



CMMC LEVEL 1 Foundational 15 Cybersecurity Practices	CMMC LEVEL 2 Advanced 110 Cybersecurity Practices	CMMC LEVEL 3 Expert 110+ Cybersecurity Practices
This Foundational level focuses on the protection of Federal Contract Information (FCI). Level 1 companies are required to self-assess and attest annually.	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.	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.

Exhibit 3. 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 support 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.

© INTERSEC, INC. ALL RIGHTS RESERVED

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 (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, if a company is dealing with controlled unclassified information (CUI) or federal contract information (FCI), 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 by the summer of 2023. 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 that 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 provide 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.

© INTERSEC, INC. ALL RIGHTS RESERVED

The CMMC Ecosystem

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

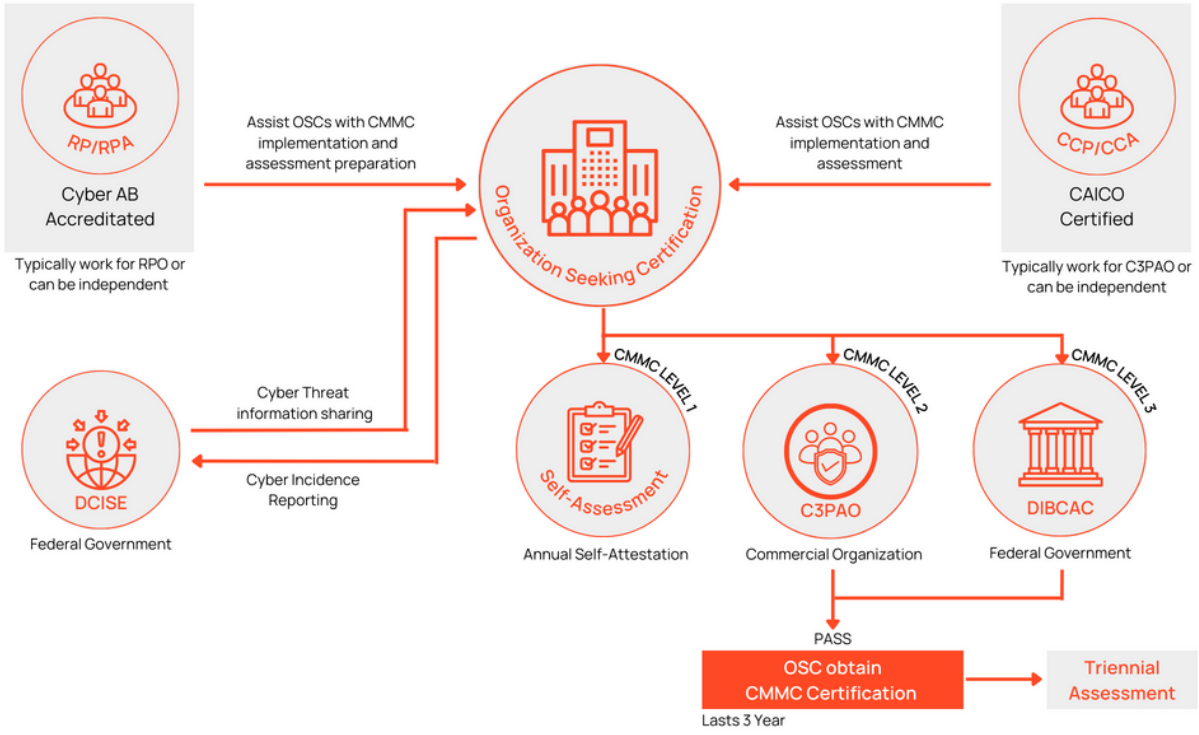


Exhibit 4 : The CMMC Ecosystem

- 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.

© INTERSEC, INC. ALL RIGHTS RESERVED

- 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.

Who does CMMC apply to?

CMMC is a requirement for all companies who want to work as a contractor with the Defense Industrial Base. Everyone involved in the defense contract supply chain, including contractors that work directly with the DoD and subcontractors who work with primes to carry out or complete contracts, must abide by the CMMC.

© INTERSEC, INC. ALL RIGHTS RESERVED

How long does it take to get CMMC certified?

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

- The first level would take between 1 to 3 months,
- The second level would take between 6 to 18 months, and
- The third level would take between 9 to 24 months.

Since it is such a long process, the earlier the company begins, the greater advantage it will have before CMMC compliance becomes law.

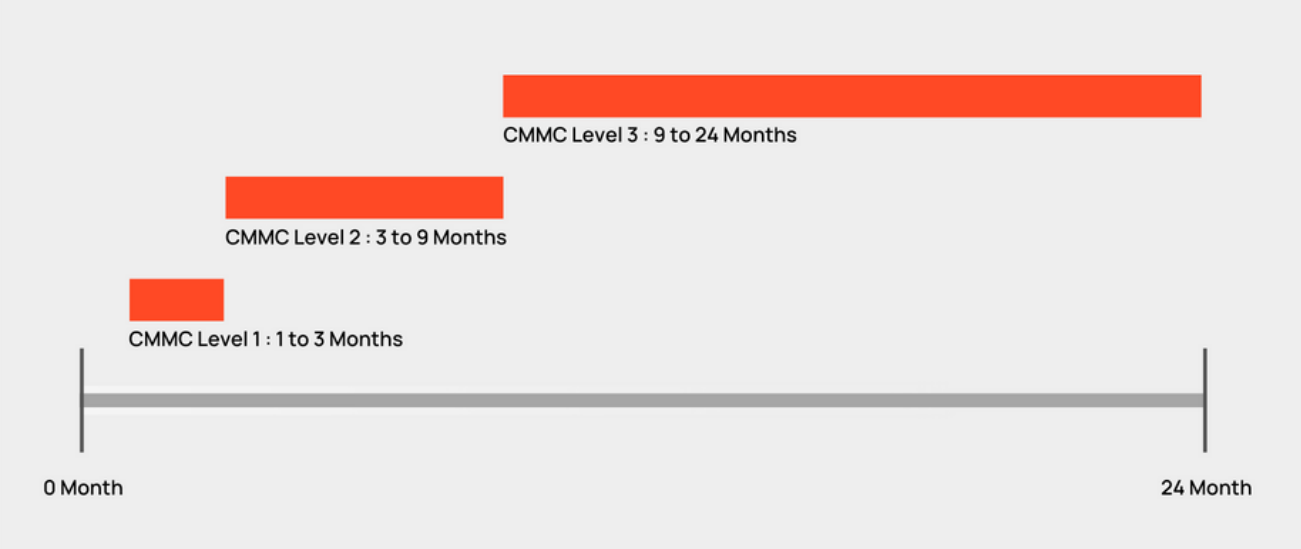


Exhibit 5 : CMMC Compliance-Start to Finish Timeline

When will CMMC requirements start appearing in solicitations?

It is predicted that in the Department of Defense's timeline, CMMC requirements could appear in solicitations in May of 2023.

Currently, CMMC compliance is a soft requirement, but it is anticipated that it will become law by May 2023. Since CMMC compliance is a long journey, currently, they allow you to bid on contracts.

However, in the future, the government will not allow companies to bid on the contract unless they are CMMC certified.

© INTERSEC, INC. ALL RIGHTS RESERVED

What CMMC level do I need?

- According to DoD, there are approximately 300,000 organizations that would require CMMC. It's estimated that 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.

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:

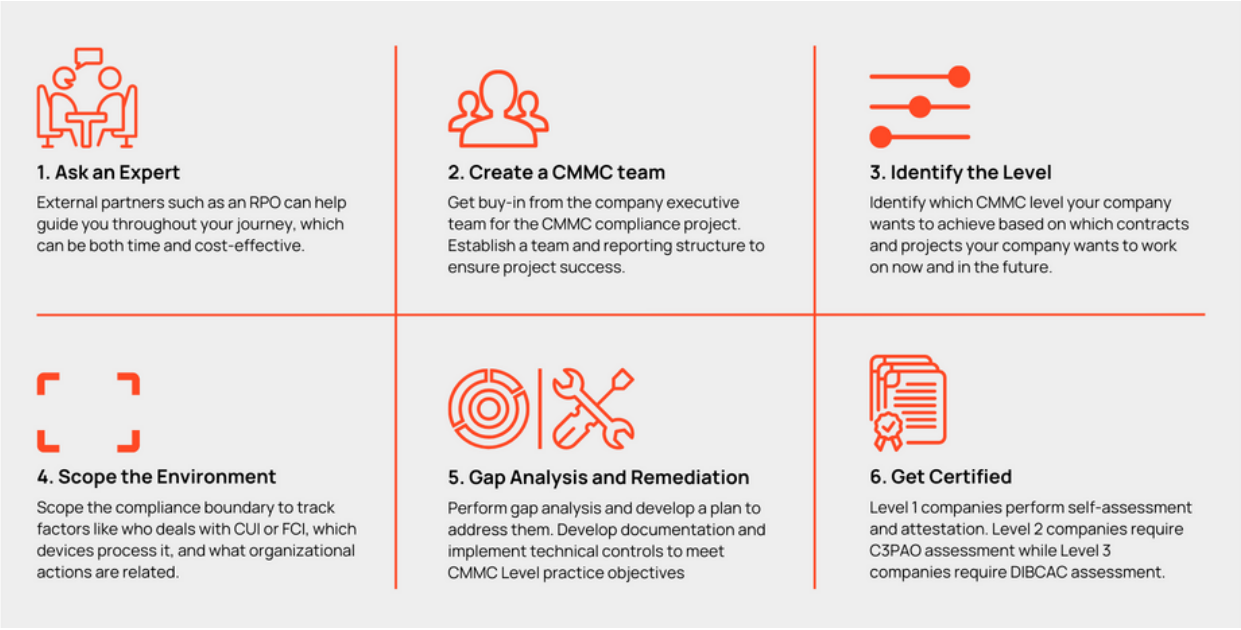


Exhibit 6. CMMC Compliance Journey

© INTERSEC, INC. ALL RIGHTS RESERVED

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, which can be both time and cost-effective.
Create a CMMC Team	Within your organization, it is important to establish a team of resourceful individuals who can explicitly focus on the CMMC's progress. These employees should be knowledgeable on the topic and able to give their time and effort to help your company become successfully CMMC certified.
Identify the Level	When beginning the CMMC journey, you must identify which CMMC level your company wants to achieve. This 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 will need to perform a gap analysis. This means investigating and understanding the company's current state and identifying the gaps that the company is missing to meet all of the requirements for CMMC. If your company is already NIST compliant, it can put your company's status ahead. After gap analysis, there is remediation. Remediation addresses the issues and gaps in the analysis and fixes and patches up the problems.
Get Certified!	For CMMC Level 1, a senior official at the organization must self-attest by signing the System Security Plan. The organization also needs to upload SPRS (Supplier Performance Risk System) score to the DoD SPRS system. For CMMC Level 2, an organization needs to find a C3PAO, a CMMC Third-Party Assessment Organization, and undergo an audit. For CMMC Level 3, an organization needs to undergo Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) audit.

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

Limited resources

Small enterprises may face difficulties in implementing security measures and fulfilling CMMC standards due to constraints such as limited financial resources, manpower, and technology.

© INTERSEC, INC. ALL RIGHTS RESERVED

Lack of expertise

Small businesses may have difficulties in comprehending and adhering to CMMC requirements due to their limited knowledge and experience in cybersecurity.

Limited access to information

Small enterprises may face challenges in obtaining information about the CMMC standard and the steps required for compliance, making the certification process difficult to navigate.

Limited access to vendors

The limited availability of credible and approved CMMC readiness vendors or individuals to assist small businesses in their journey towards CMMC compliance.

Limited budget

The restricted financial resources of small businesses may pose a challenge in meeting the expenses associated with compliance and certification under the CMMC standard.

Exhibit 7 : Challenges faced by Small Business to comply with CMMC

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.

© INTERSEC, INC. ALL RIGHTS RESERVED

The image below shows assessment requirements under CMMC 2.0

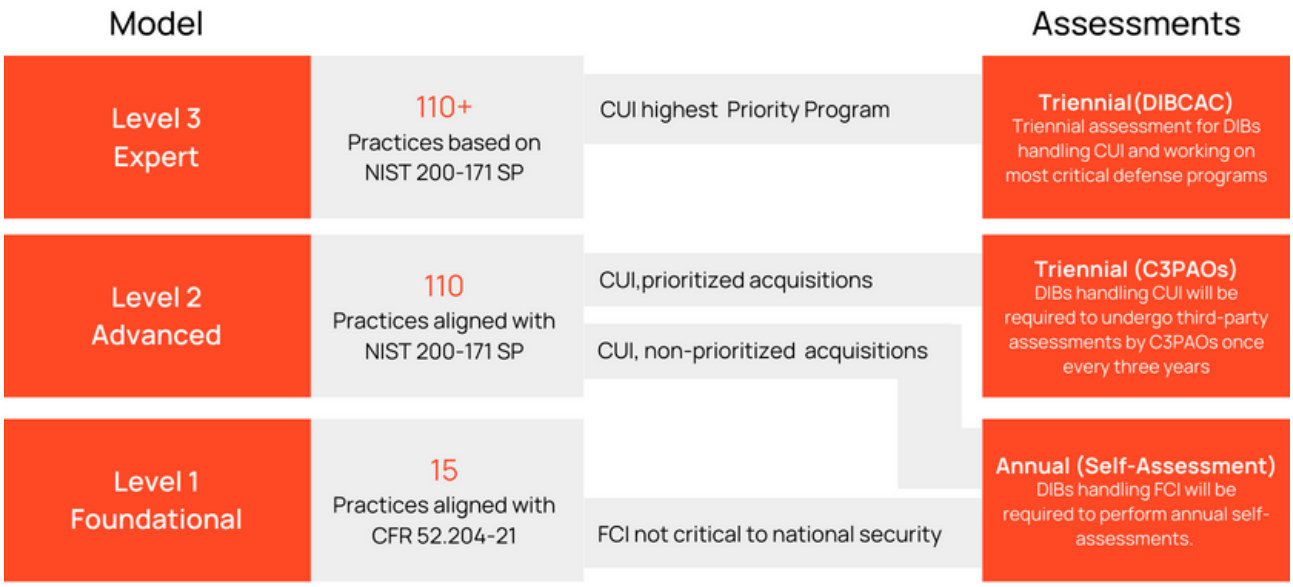


Exhibit 8 : Assessment requirements under CMMC 2.0

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.

© INTERSEC, INC. ALL RIGHTS RESERVED

Which controls are consistently failing DIBCAC assessments?

Around November of 2022, DIBCAC Director for the Defense Contract Management Agency (DCMA), Nick DelRosso, 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.

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.

What is an 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.

© INTERSEC, INC. ALL RIGHTS RESERVED

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.

© INTERSEC, INC. ALL RIGHTS RESERVED

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.

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.

(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
	-Mobile Device Support	
3. Office 365 Implementation to CMMC L2	-Full Desktop Support	3. Duo Federal
4. Azure Implementation to CMMC L2	-Full 24 x 7 helpdesk	4. Email/Drive encryption license
5. MFA to the Desktop built to CMMC L2		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 9 : Sample Cost Components

© INTERSEC, INC. ALL RIGHTS RESERVED

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 rulemaking 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.

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.

Exhibit 10 : Factors affecting the cost of compliance

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 assessments.

© INTERSEC, INC. ALL RIGHTS RESERVED

How can an RPO like InterSec 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.

RPOs can assist with the assessment process, provide training and resources, and offer feedback and recommendations for improvement. Partnering with an RPO 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

© INTERSEC, INC. ALL RIGHTS RESERVED

InterSec
Ignite . Inspire. Innovate

Case Study 1 : Unleashing cybersecurity 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.

© INTERSEC, INC. ALL RIGHTS RESERVED

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.

© INTERSEC, INC. ALL RIGHTS RESERVED

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 us 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

© INTERSEC, INC. ALL RIGHTS RESERVED

InterSec
Ignite . Inspire. Innovate

CMMC COMPLIANCE CONSULTING FOR DOD CONTRACTORS

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 CMMC-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
• SCOPING TO EVALUATE APPLICABLE CMMC LEVEL • IDENTIFY CUIS, FCIS • ESTABLISHING EXISTING CYBERSECURITY MATURITY • ASSESS COMPLIANCE • SPRS EVALUATION • POA&MS WITH ACTIONABLE REMEDIATION GUIDANCE	• DOCUMENTATION AND TECHNICAL REMEDIATION • ESTABLISHING EXISTING CYBERSECURITY MATURITY • ASSESS COMPLIANCE • SPRS SCORE • POA&M • SYSTEM SECURITY PLAN • ACTIONABLE REMEDIATION REPORT	• PERIODIC POLICIES AND PROCEDURES REVIEWS AND UPDATES • INCIDENT RESPONSE TABLE TOP EXERCISE • ANNUAL PHISHING EXERCISES • SECURITY AWARENESS TRAINING • PERIODIC VULNERABILITY SCAN • SPRS SCORE UPDATES

© INTERSEC, INC. ALL RIGHTS RESERVED

InterSec
Ignite . Inspire. Innovate

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

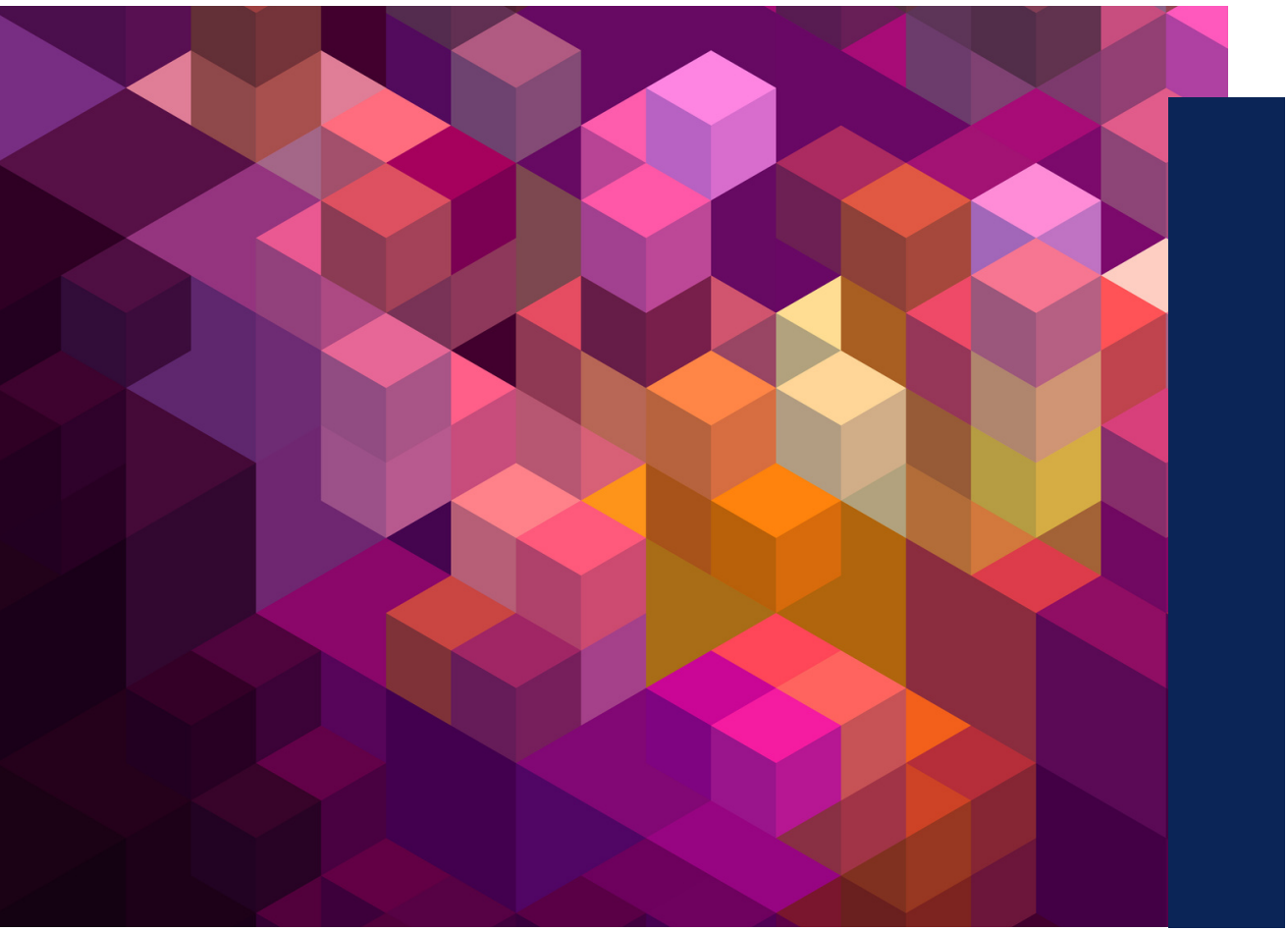
Hundreds of DFARS assessments and readiness experience

170+ NIST 800-171 SSP, POA&M, AND SPRS	200+ LEVEL 1 ADVISORY AND CONSULTING	50+ LEVEL 2 ADVISORY, CONSULTING, AND MSSP

OUR CLIENTS

© INTERSEC, INC. ALL RIGHTS RESERVED

InterSec
Ignite . Inspire. Innovate



InterSec
Ignite . Inspire. Innovate

Ready to start your CMMC Journey?

Please contact us at complianceservices@intersecinc.com
Call us at (833) 228-4858 (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.