# CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

## Frequently Asked Questions

One PPG Place, Suite 1700
Pittsburgh, PA 15222
(412) 697-5200
www.schneiderdowns.com

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

# In This Document

As part of our continued commitment to helping organizations prepare for CMMC, we are curating some of the most relevant frequently asked questions from authorized resources and professionals for quick reference. Questions include:

- What is CMMC?
- What is Controlled Unclassified Information (CUI)?
- Why was CMMC created?
- When is the interim Defense Federal Acquisition Regulation Supplement (DFARS) rule implementing CMMC (DFARS Case 2019-D041) effective?
- What is the relationship between National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 and CMMC?
- How will CMMC be different from NIST SP 800-171?
- Will there be a self-certification?
- How often does my organization need to be reassessed?
- My organization does not handle Controlled Unclassified Information (CUI). Do I have to be certified anyway?
- I am a subcontractor on a DoD contract. Does my organization need to be certified?
- How will I know what CMMC level is required for a contract?
- What is the Department's phased rollout plan for CMMC?
- How is the CMMC framework organized?
- What are maturity processes and how do they fit into the CMMC framework?
- What are practices and how do they fit into the CMMC framework?
- What Domains Are Included in the CMMC Framework?
- What is the DFARS Interim Rule and how does it impact CMMC and DOD prime and subcontractors?
- How do you pass CMMC certification assessment?
- What happens if your C3PAO determines that a practice has not been implemented sufficiently?
- What organizations make up the CMMC ecosystem?
- What CMMC certification level is required for prime and subcontractors that possess CUI?
- When will an organization need to be CMMC certified?
- How should an organization prepare for CMMC certification?
- How will third parties such as managed security providers (MSPs) and cloud service providers (CSPs) impact an organizations CMMC certification requirements?
- What type of evidence is required to prove that each practice has been implemented?
- What is Federal Contract Information (FCI)?
- How much will a CMMC assessment cost?
- Do you need to use GCC High to meet CMMC requirements?
- Are prime contractors and subcontractors required to complete a NIST 800-171 self-assessment in the Supplier Performance Risk System (SPRS) since the DFARS interim rule went into effect on November 30, 2020?
- Should I enter my self-assessment into SPRS even if my score is low or even negative?
- Are prime contractors required to flow down requirements to their subcontractors for completing a self-assessment in SPRS?
- As a subcontractor, are we required to comply with our prime contractor's request for us to complete a self-assessment in SPRS?
- What will reciprocity look like for companies who have already achieved FedRAMP authorization?

# What is CMMC?

CMMC stands for "Cybersecurity Maturity Model Certification" and is a unifying standard for the implementation of cybersecurity across the Defense Industrial Base (DIB). The CMMC framework includes a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. CMMC is designed to provide increased assurance to the Department that a DIB company can adequately protect sensitive unclassified information, accounting for information flow down to subcontractors in a multi-tier supply chain.

# What is Controlled Unclassified Information (CUI)?

CUI is 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.

CUI is a newer term developed for all Executive Branch Agencies. Prior to the establishment of the term "CUI", each agency used their own internal terminology to describe the same information. Some of these retired terms would be: Unclassified Controlled Technical Information (UCTI), For Official Use Only (FOUO), Sensitive but Unclassified (SBU), and others.

CUI encompasses two other classifications of data: Covered Defense Information (CDI) and Controlled Technical Information (CTI). CDI is information that is marked and subject to the protections outlined within DFARS Clause 252.204-7012. CTI is any technical information with a military or space application that is subject to the protections within DoDI 5230.24. All CDI and CTI are CUI, but not all CUI is CDI or CTI. A CUI Registry provides information on the specific categories and subcategories of information that the Executive branch protects. The CUI Registry can be found at: www.archives.gov/cui and www.dodcui.mil/Home/DoD-CUI-Registry/ and includes the following organizational index groupings:

- Critical Infrastructure
- Defense
- Export Control
- Financial
- Immigration
- Intelligence
- International Agreements
- Law Enforcement
- Legal
- Natural and Cultural Resources
- NATO
- Nuclear
- Privacy
- Procurement and Acquisition
- Proprietary Business Information
- Provisional
- Statistical
- Tax

Resources, including online training to better understand CUI can be found on National Archives' website at www.archives.gov/cui/training.html as well as the Department of Defense's website www.dodcui.mil/.

# Why was CMMC created?

The Department of Defense (DoD) is migrating to the new CMMC framework in order to assess and enhance the cybersecurity posture of the Defense Industrial Base (DIB) sector. The CMMC is intended to serve as a verification

mechanism to ensure that DIB companies implement appropriate cybersecurity practices and processes to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within their unclassified networks.

## When is the interim Defense Federal Acquisition Regulation Supplement (DFARS) rule implementing CMMC (DFARS Case 2019-D041) effective?

The interim rule became effective on November 30, 2020. The public review and comment period for DFARS Case 2019-D041 ended on November 30, 2020. Due to its designation as a major rule change, the interim rule must also complete a Congressional Review.

## What is the relationship between National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 and CMMC?

CMMC Level 3 includes the 110 security requirements specified in NIST SP 800-171. The CMMC Model also incorporates additional practices and processes from other standards, references, and/or sources such as NIST SP 800-53, Aerospace Industries Association (AIA) National Aerospace Standard (NAS) 9933 "Critical Security Controls for Effective Capability in Cyber Defense", and Computer Emergency Response Team (CERT) Resilience Management Model (RMM)..

## How will CMMC be different from NIST SP 800-171?

Unlike NIST SP 800-171, the CMMC model possesses five levels. The model is cumulative whereby each level consists of practices and processes as well as those specified in the lower levels. The CMMC Model includes additional cybersecurity practices in addition to the security requirements specified in NIST SP 800-171. In addition to assessing a company's implementation of cybersecurity practices, the CMMC will also assess the company's maturity processes.

## Will there be a self-certification?

No, there are no self-certifications for CMMC. However, DIB companies are encouraged to complete a self-assessment based on CMMC Assessment Guides prior to scheduling a CMMC assessment. The Department of Defense posts versions of the CMMC Assessment Guides on its website.

## How often does my organization need to be reassessed?

In most cases, a CMMC certificate will be valid for 3 years.

## My organization does not handle Controlled Unclassified Information (CUI). Do I have to be certified anyway?

If a DIB company does not possess, store, or transmit CUI but possesses Federal Contract Information (FCI), it is required to meet FAR clause 52.204-21 and must be certified at a minimum of CMMC Level 1. Companies that solely produce Commercial-Off-The-Shelf (COTS) products do not require a CMMC certification.

## I am a subcontractor on a DoD contract. Does my organization need to be certified?

If the DoD contract has a CMMC requirement and so long as your company does not solely produce COTS products, you will need to obtain a CMMC certificate. The level of the CMMC certificate is dependent upon the type and nature of information flowed down from your prime contractor.

## How will I know what CMMC level is required for a contract?

The DoD will specify the required CMMC level in Requests for Information (RFIs) and Requests for Proposals (RFPs).

## What is the Department's phased rollout plan for CMMC?

The Department is implementing CMMC through a phased rollout approach. Until September 30, 2025, the Office of the Under Secretary of Defense for Acquisition and Sustainment must approve the inclusion of the CMMC requirement in any solicitation.

The Department is currently working with military Services and Defense Agencies to identify candidate programs that will implement CMMC requirements during the FY2021-FY2025 phased rollout. During the first year of the rollout, the Department will require no more than 15 new Prime acquisitions to meet CMMC requirements as part of a CMMC pilot program. These contracts will focus on mid-sized programs that require the contractor to process or store CUI (CMMC Level 3). Primes will be required to flow down the appropriate CMMC requirement to their subcontractors.

For subsequent fiscal years of the rollout, the Department intends to incorporate CMMC Levels 4 and 5 on a small number of contracts while increasing the quantity of Prime acquisitions that include a CMMC requirement to the following targets:

| FY2021 | FY2022 | FY2023 | FY2024 | FY2025 |
|---|---|---|---|---|
| 15 | 75 | 250 | 325 | 475 |

The full list can be found at www.acq.osd.mil/cmmc/faq.html.

## How is the CMMC framework organized?

The CMMC framework consists of maturity processes and cybersecurity best practices from multiple cybersecurity standards, frameworks, and other references, as well as inputs from the DIB and DoD stakeholders. The model framework organizes these processes and practices into a set of domains and maps them across five levels. In order to provide additional structure, the framework also aligns the practices to a set of capabilities within each domain.

## What are maturity processes and how do they fit into the CMMC framework?

The CMMC model consists of five maturity processes that span Maturity Levels (ML) 2-5 and apply to all domains.

## What are practices and how do they fit into the CMMC framework?

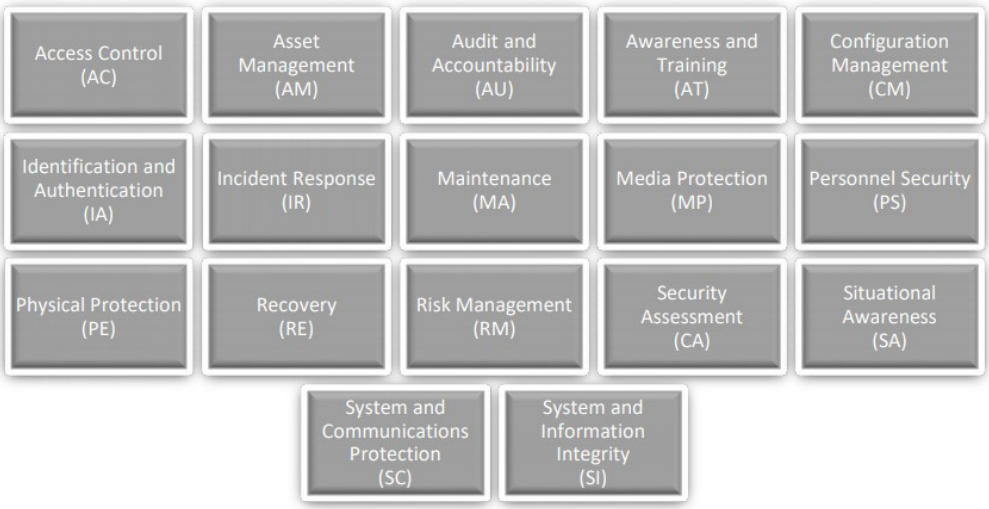
Practices are synonymous with controls. The CMMC framework consists of 171 practices that are mapped across the five levels for all capabilities and domains.

The majority of practices (110 of 171) originate from the safeguarding requirements and security requirements specified in FAR Clause 52.204-21 and DFARS Clause 252.204-7012. Level 1 is equivalent to all the safeguarding requirements from FAR Clause 52.204-21. Level 3 includes all of the security requirements in NIST SP 800-171 plus 20 additional practices. The remaining practices stem from multiple references as well as inputs from the DIB and DoD stakeholders.

| CMMC Level | Number of Practices Introduced at CMMC Level | Source | | | |
|---|---|---|---|---|---|
| | | 48 CFR 52.204-21 | NIST SP 800-171r1 | Draft NIST SP 800-171B | Other |
| 1 | 17 | 15* | 17* | - | - |
| 2 | 55 | - | 48 | - | 7 |
| 3 | 58 | - | 45 | - | 13 |
| 4 | 26 | - | - | 11 | 15 |
| 5 | 15 | - | - | 4 | 11 |
| **Total** | **171** | **15** | **110** | **15** | **46** |

## What Domains Are Included in the CMMC Framework?

The CMMC framework consists of 17 domains. The majority of these domains originate from the security-related areas in Federal Information Processing Standards (FIPS) Publication 200 and the related security requirement families from NIST SP 800-171. The CMMC framework also includes three additional domains of Asset Management (AM), Recovery (RE), and Situational Awareness (SA).




To download the full CMMC Model V1.02 Guide, please visit www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

## What is the DFARS Interim Rule and how does it impact CMMC and DOD prime and subcontractors?

The DFARS Interim Rule is a rule issued by the Department of Defense that went into effect on December 1, 2020. The new rule applies to all contractors who are subject to DFARS 252.204-7012 clause, which is based on the contractors handling CUI. The rule will therefore apply to all DoD primes and subcontractors who are in possession of CUI. The DFARS Interim Rule will be in effect from December 1,2020 until the successful implementation of CMMC in the next 5 years. This Interim Rule includes three new clauses:

- DFARS 252.204-7019
- DFARS 252.204-7020
- DFARS 252.204-7021

DFARS Clause 252.204-7019 outlines a requirement that all contractors (primes and their subcontractors) that handle CUI must complete a new NIST 800-171 Self-Assessment, which contains a new scoring methodology, and post this self-assessment score in the DoD's Supplier Performance Risk System (SPRS). The assessments must be completed, and scores posted before a contract can be awarded to a contractor. The self-assessment also requires a completed System Security Plan (SSP) and a Plan of Action and Milestones (POAM) for all 800-171 requirements that are currently not being met by the contractor's system.

Finally, the Defense Contract Management Agency (DCMA) will be conducting random audits of these self-assessments to ensure that primes and their subcontractors are accurately self-assessing their systems.

DFARS Clause 252.204-7020 states that the DoD will conduct the assessments for Medium or High-risk contractors. The clause itself outlines this process. Contractors are required to provide the DoD with access to their facilities, systems, and personnel for the DoD to conduct these assessments. The DoD will then post the summary of these scores within the SPRS (e.g., 100 out of 110 requirements met) as well as an expected implementation date for all requirements to be implemented. The contractor in question will then have 14 days to rebut any findings in question and/or provide evidence for controls that could not be assessed by the DoD during the initial assessment. The contractor also must insert the substance of this clause into all subcontracts.

Finally, DFARS Clause 252.204-7021 defines the scope and requirements for the CMMC itself. This clause includes the definition of a current CMMC score (No older than 3 years), the requirement to maintain CMMC certification throughout the duration of the contract, and the requirement for subcontractors to also maintain a CMMC certification.

## How do you pass CMMC certification assessment?

The answer to this question depends on what level of CMMC assessment you are required to undergo. The requirements for a Level 1 assessment are significantly different from the requirements for a Level 3 assessment, which are significantly different from a Level 5 assessment. A Level 1 assessment consists of 17 CMMC Practices which must be met before CMMC certification can be awarded. A Level 2 assessment is 72 total CMMC Practices, a Level 3 consists of 130 total CMMC practices, a Level 4 is 156 total CMMC Practices, and a Level 5 consists of 171 total CMMC Practices. The best place to determine what Level of CMMC assessment your organization will require is the specific contract that is being bid on, which going forward, should include a required level. However, for contracts already in place, if you are a prime or subcontractor for a prime in possession of DoD CUI, you will at least need a Level 3 assessment.

With that said, there is currently no way to pass a CMMC assessment. A CMMC assessment must be completed by a C3PAO, who themselves need to undergo CMMC certification. At the time of writing, there are no C3PAO firms authorized to conduct a CMMC assessment, which is where DFARS Interim Rule comes into play. In the meantime, to prepare your organization for a CMMC assessment, your organization should examine the latest CMMC documentation and determine which CMMC practices are in place, and which are still being implemented. All practices within the CMMC assessment your organization is undergoing must be implemented prior to the assessment. To achieve certification, all practices at the CMMC level being assessed must be in place in order to be certified and the CMMC does not allow for Plans of Actions & Milestones (POA&Ms). The CMMC-AB does however allow for a 90-day remediation period, wherein a contractor has 90 days to remediate any findings identified by the C3PAO. If a practice is not in place after 90 days, the Organization Seeking Certification must restart the CMMC assessment process

## What happens if your C3PAO determines that a practice has not been implemented sufficiently?

If your C3PAO has determined that a practice has not been sufficiently implemented, as currently outlined by the CMMC AB, your organization will have a period of 90 days to remediate these practices and conform to the CMMC practice. But not all practices are equal in terms of their difficultly to remediate. For some gaps, this 90-day period may be sufficient for remediation, but other practices may take longer. In the event that a gap cannot be remediated within 90 days, your organization will have to reapply for an assessment after the gap has been addressed and begin the CMMC certification process again.

| Acronym | Full Name | Function within CMMC Ecosystem |
|---|---|---|
| DoD | Department of Defense | Created the CMMC Framework |
| DIB | Defense Industrial Base | The organizations that the DoD uses as an industrial asset, of direct or indirect importance for producing equipment or services for the Nation's armed forces. |
| CMMC-AB | CMMC Accreditation Body | Validates CMMC assessments and credentials organizations within the CMMC Ecosystem |
| CAICO | CMMC Assessors and Instructors Certification Organization | Arm of the CMMC-AB that is responsible for training and certifying assessors |
| RPO | Registered Provider Organization | Organizations that can performing consulting work related to the CMMC framework |
| RP | Registered Practitioner | Employee at an RPO who performs the consulting work |
| C3PAO | CMMC Third-Party Assessor Organization | Organizations that can perform CMMC assessments. |
| OSC | Organization Seeking Certification | Organization that is undergoing a CMMC assessment. |
| CP | Certified Professional | Can participate in a CMMC assessment under the supervision of CA-1 and higher-level assessor |
| CA-1 | Certified CA-1 Assessor | Can perform a CMMC ML-1 assessment and supervise a CP |
| CA-3 | Certified CA-3 Assessor | Can perform a CMMC ML-1 or ML-3 assessment and supervise a CA-1 or lower-level assessor |
| CA-5 | Certified CA-5 Assessor | Can perform any level of CMMC assessment and supervise any level of assessor |

## What CMMC certification level is required for prime and subcontractors that possess CUI?

The level required for CMMC that prime and subcontractors will need to meet will be dependent on their contracts and the information they obtain from the government. If an organization possesses CUI, the organization will be required to be at least CMMC level 3, however the Department of Defense has indicated that they will specify the required CMMC level in both Requests for Information and Requests for Proposals. Depending on the type of CUI, organizations may be required to be certified at level 4 or 5.

## When will an organization need to be CMMC certified?

An organization will need to be certified at the required CMMC level specified in the contract to obtain the contract for work from the DoD. The DoD has indicated it plans to do a phased rollout of CMMC requirements within prime contracts starting in FY21 with approximately 15 pilot contracts, continuing to increase that roll out over the next 5 years, including rolling out CMMC level 5 requirements in contracts starting in FY22. As it currently stands, all DOD prime and subcontractors will need to be CMMC certified at the appropriate level specified in their contracts by 2026.

## How should an organization prepare for CMMC certification?

As the CMMC certification requires all controls in place and operating effectively to be certified, we recommend working with an independent party that has CMMC experience prior to engaging in the CMMC assessment. The independent party can perform a gap or readiness assessment to determine if you are meeting the controls at your desired CMMC level before you attempt the certification review.

Before working with an independent party to perform a gap or readiness assessment, it is critical to review the CMMC level 1 and CMMC level 3 assessment guides, which can be found at: www.acq.osd.mil/cmmc/draft.html. These guides will provide the required background knowledge for your organization to determine which CMMC practices the organization needs to meet for the level of CMMC certification being sought. Within these assessment guides are the specific CMMC practices that must be in place as well as the processes that must be in place to support these practices. Policies should be written to fulfill these processes. As an example, the process to support Access Control (AC) practices states that organizations must "Establish a policy that includes Access Control".

Finally, the entire IT environment does not require CMMC assessment and certification. Only portions of the environment that store, process, transmit, or receive CUI and FCI are required to undergo CMMC certification. Therefore, your organization should analyze the environment to determine which portions of the environment contain CUI and FCI. To simplify the implementation of CMMC practices and CMMC assessment, the portions of the environment containing CUI and FCI can be isolated within a network enclave. Segmenting this portion of the network or system from the general IT environment will reduce the scope of the assessment and simplify the implementation of CMMC practices.

## How will third parties such as managed security providers (MSPs) and cloud service providers (CSPs) impact an organizations CMMC certification requirements?

A contractor can inherit practice objectives. A practice objective that is inherited is met because adequate evidence is provided that the enterprise or another entity, such as an External Service Provider (ESP), performs the practice objective. Evidence from the enterprise or the entity from which the objectives are inherited should show they are applicable to in-scope assets and that the assessment objectives are met. For each practice objective that is inherited, the Certified Assessor includes statements that indicate how they were evaluated and from whom they are inherited. If the contractor cannot demonstrate adequate evidence for all assessment objectives, through either contractor evidence or evidence of inheritance, the contractor will receive a "NOT MET" for the practice.

## What type of evidence is required to prove that each practice has been implemented?

There are three types of objective evidence that are recognized by the assessor. For each practice, two out of the following types of evidence will be required:

1. **Examine**: The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects or artifacts to facilitate understanding, achieve clarification, or obtain additional evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time. For an artifact to be accepted as evidence in an assessment, it must demonstrate the extent of implementing, performing, or supporting the organizational or project processes that can be mapped to one or more CMMC practices and those artifacts must be produced by people who implement or perform the processes.

2. **Interviews**: The process of conducting discussions with individuals or groups of individuals in an organization to facilitate understanding, achieve clarification, or lead to the location of evidence. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time. For an interview statement to be accepted as evidence in an assessment, it must demonstrate the extent of implementing, performing, or supporting the host, supporting function or enclave processes that can be mapped to one or more CMMC model practices; interview affirmations must be provided by people who implement, perform, or support processes.

3. **Tests**: The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior. The results are used to support the determination of security safeguard existence, functionality, correctness, completeness, and potential for improvement over time and institutionalization. For a test/demonstration to be accepted as evidence in an assessment, it must pass its requirements and criteria while being observed by the CA and assessment team. Any failed test results in a failed CMMC practice/control or process.

## What is Federal Contract Information (FCI)?

FCI is information that is not meant to be released to the public and is provided by or created for the Government under a contract during the development or delivery of a product or service. FCI does not include information that the Government provides to the public, such as the data on public Government websites, or transactional data used to

process payments by the Government. If your organization is only in possession of FCI and not CUI, you will only need a Level 1 assessment performed.

## How much will a CMMC assessment cost?

The answer to this question depends on a number of factors. First and foremost is the level of CMMC certification that your organization requires. A CMMC ML-1 assessment consists of 17 CMMC practices and an ML-5 assessment consists of 171 CMMC practices. Because of the differences in the number of practices being assessed at each level of CMMC certification, a higher-level assessment will cost more than a lower level CMMC assessment. The second factor that will have a direct effect on the cost of the assessment is the scope and complexity of the environment being assessed. A relatively simple system or network segment will cost level overall to assess than a situation where the C3PAO must assess the entire IT environment. Katie Arrington, Chief Information Security Officer for the Acquisition Office of the DoD has estimated that a level 1 CMMC assessment could cost as little as $3,000-$5,000, however, these numbers are only estimates based upon the currently outlined CMMC requirements. As these requirements change, so will these estimates, where they may increase or decrease.

In addition to the certification assessment cost, organizations will also have to consider costs associated with preparing for a CMMC assessment (i.e. consultants, gap analysis, etc.) and purchasing technology necessary for meeting CMMC requirements (i.e. SIEM tools, Firewalls, etc.).

The more important item to note is that for current DoD contractors, the cost of the CMMC assessment and remediations that fall under the 90-day remediation period are considered as allowable costs by the DoD. This means that current defense contractors are able to be reimbursed for the cost of having the assessment performed and validating the remediation efforts. It is critical to note, however, that the initial costs of actually getting the environment ready for the CMMC assessment are not considered allowable costs at this time and will be paid fully by the Organization Seeking Certification.

## Are prime contractors and subcontractors required to complete a NIST 800-171 self-assessment in the Supplier Performance Risk System (SPRS) since the DFARS interim rule went into effect on November 30, 2020?

Beginning on November 30, 2020, contracting officers will have to confirm that an organization has an active SPRS assessment in its system before awarding a new contract or exercising an option under an existing contact where the contractor or offeror is required to implement NIST 800-171. The assessment in SPRS cannot be older than three years. Based on the above, November 30, 2020 is not a deadline for every contractor and subcontractor. However, if you are a prime contractor and you are planning to bid on a new contract with DFARS 252.204-7012 included or a current contract with DFARS 252.204-7012 included that has an exercise option looming, then it is highly recommended that you complete a self-assessment in SPRS system as soon as possible.

## Should I enter my self-assessment into SPRS even if my score is low or even negative?

It is unclear on how the DoD will use the scores entered in SPRS when awarding contracts and if the actual score will impact decisions. Since contracting officers will have to confirm that an organization has an active SPRS assessment

in its system before awarding a new contract or exercising an option under an existing contact, it is recommended to complete a self-assessment in SPRS even if the score is low or even negative. Contractors without scores in SPRS bidding on new contracts with DFARS 252.204-7012 included, will not be considered when the contract is awarded.

## Are prime contractors required to flow down requirements to their subcontractors for completing a self-assessment in SPRS?

Yes – prime contractors will be required to confirm that all subcontractors included a contract they are bidding on have an active score in SPRS.

## As a subcontractor, are we required to comply with our prime contractor's request for us to complete a self-assessment in SPRS?

Technically, you are not required to complete a self-assessment in SPRS unless you are bidding on a new contract with your prime contractor that includes DFARS 252.204-7012 or if your prime contractor's contract that includes DFARS 252.204-7012 has an exercise option looming.

Most prime contractors are planning for future contracts and are currently requiring all their subcontractors to complete self-assessments in SPRS. Considering how many subcontractors prime contractors may work with, it makes sense that prime contractors would require this, since they do not want to be overlooked for future contracts because their subcontractors do not have an active scores in SPRS.

## What will reciprocity look like for companies who have already achieved FedRAMP authorization?

There are plans for CMMC to provide reciprocity to organizations that have successfully completed a FedRAMP certification. However, there has not been an official policy document outlined on when this will happen or how it will work.

SCHNEIDER DOWNS
Big Thinking. Personal Focus.

# CYBERSECURITY MATURITY MODEL CERTIFICATION
# PREPARATION CHECKLIST

## 12 months PRIOR

One year out from a Cybersecurity Maturity Model Certification (CMMC) engagement, your organization should begin to lay the groundwork for an engagement by determining your internal team who will be responsible for the CMMC process and evaluating where both Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) are processed and reside within the environment. Your organization should determine if a readiness assessment for the CMMC assessment will be performed in-house or with assistance from a third party.

- ☐ Assign responsibility for managing the CMMC process internally.
- ☐ Review all your current Department of Defense (DoD) contracts, subcontracts, and agreements for FCI/CUI/CMMC-based requirements.
- ☐ Evaluate potential contract bids for FCI/CUI/CMMC-based requirements.
- ☐ Evaluate where FCI and CUI reside, and any data flows associated with them.
- ☐ Determine a process to perform a readiness assessment against the required CMMC level, dependent on your DoD contracts.
  - ☐ Evaluate if a third party should be used for the readiness and start reaching out for an assessment.
  - ☐ If performing the readiness assessment in-house, determine a team and approach.

## 9 months PRIOR

Nine months prior to the assessment, your organization should be in the process of performing a readiness assessment and determining potential gaps against the CMMC control standards. Any gaps should have a roadmap created to resolve the issue with actionable milestones.

- ☐ Perform the readiness assessment aligning to the CMMC standards and evaluate your internal environment for potential gaps.
  - ☐ Identify control owners and subject matter experts.
  - ☐ Depending on gaps or weaknesses identified, develop a project timeline and roadmap to remediate any issues.
- ☐ If required by your DoD contract, establish a Supplier Performance Risk System (SPRS) account within the DoD systems.

## 6 months PRIOR

Six months prior to the assessment, your organization should continue to remediate any gaps detected and ensure timelines are being met. Additionally, your organization should start to evaluate CMMC Third Party Assessor Organizations (C3PAO's) to perform the assessment based on the CMMC guidelines.

- ☐ Continue to monitor project roadmap and ensure milestones are met for remediation.
- ☐ If required by your DoD contract, submit your self-assessment score into the SPRS system.
- ☐ Contact and evaluate potential C3PAO's to perform the CMMC assessment.

## 3 months PRIOR

Three months prior to the assessment, your organization should have selected a C3PAO and should be coordinating the approach, assessment timetable, and key contacts to perform the assessment. In addition, your organization should ensure that all the gaps detected from the readiness have been or will be remediated by the time the assessment starts.

- ☐ Continue to monitor project roadmap and ensure milestones are met for remediation.
- ☐ Select and coordinate planning of CMMC assessment approach and timing with C3PAO.

### How Can Schneider Downs Help?

Schneider Downs is a Candidate C3PAO. Our team currently offers CMMC readiness and consulting services as a Registered Provider Organization (RPO). Our team includes a Certified CMMC Provisional Assessor, and several other members currently in process of applying for CMMC Certified Assessor status who plan on completing training in Q2 of 2021. OSCs should note that a single firm cannot perform both consulting and audit services for a single client per the CMMC-AB standards. In the meantime, until such requirements are made public, we can help your organization prepare for CMMC by performing an assessment against the NIST 800-171 framework.

For more information visit www.schneiderdowns.com/cmmc or contact us at contactsd@schneiderdowns.com.


SCHNEIDER DOWNS
Big Thinking. Personal Focus.

www.schneiderdowns.com

**PITTSBURGH**
One PPG Place
Suite 1700
Pittsburgh, PA 15222
P 412.261.3644

**COLUMBUS**
65 E. State Street
Suite 2000
Columbus, OH 43215
P 614.621.4060

**WASHINGTON, D.C.**
1660 International Drive
Suite 600
McLean, VA 22102
P 571.380.9003

SCHNEIDER DOWNS
Consulting

# Consulting Services

# CYBERSECURITY MATURITY MODEL CERTIFICATION SERVICES

The Cybersecurity Maturity Model Certification (CMMC) is a unified standard for implementing cybersecurity across the defense industrial base (DIB), which includes hundreds of thousands of contractors across the nation. The Department of Defense created the CMMC compliance standard to improve the security of the supply chain of the DIB.

## SCHNEIDER DOWNS QUALIFICATIONS

### Certified Third-Party Assessor Organization (C3PAO)

We are approved as a C3PAO by the CMMC Accreditation Body (CMMC-AB) and have completed the organization background checks required by the CMMC-AB. We are scheduling our CMMC Level 3 assessment with the Department of Defense (DoD) and once we are CMMC Level 3 certified, we will be authorized to perform CMMC certifications assessments.

### Registered Provider Organization (RPO)

We are authorized as an RPO by the CMMC-AB to provide CMMC advisory and consulting services to assist clients in preparing for CMMC certification assessments.

### Provisional Assessor

We currently employ one of only 100 CMMC provisional assessors in the United States. As part of the Provisional Assessor program, we are helping shape the future of the CMMC program by providing valuable feedback and insight to the CMMC-AB.

### Registered Practitioners (RP)

We currently employ RPs that have completed the CMMC-AB's RP training and passed the required the background checks.

### Certified CMMC Professionals (CCP) and Certified CMMC Assessors (CCA)

Several members of our IT and Cybersecurity Risk Advisory team have applied to be CCPs and CCAs through the CMMC-AB application process and will complete required training and examinations once these are made available to us by the Licensed Training Providers.

## SCHNEIDER DOWNS CMMC SERVICES

Schneider Downs currently provides CMMC readiness and consulting services including:

### C3PAO Services

Once we pass our CMMC level 3 assessment, we will be authorized to perform CMMC certification assessment services as a C3PAO.

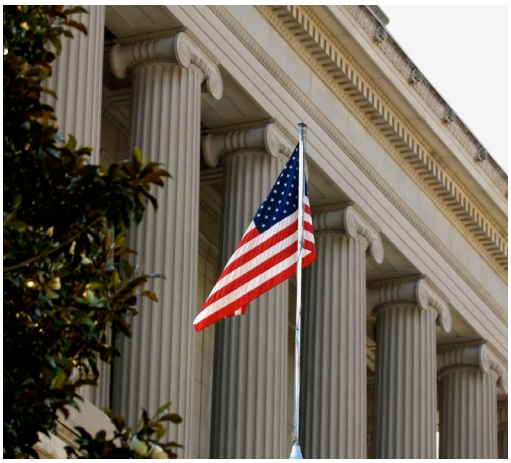
### RPO Services

As an RPO, we perform the following CMMC services:

- *CMMC Program Management* – Development of a CMMC program roadmap and ongoing program management to ensure that key milestones are adequately met in preparation for a CMMC

certification assessment from a C3PAO. Evaluation of the defined scope of the CUI/FCI boundary to determine if the CUI/FCI is appropriately identified and isolated. Development of the System Security Plan (SSP).

- *CMMC Readiness Assessment* – Review of the SSP, CUI/FCI boundary, policies, procedures, processes and artifacts to determine if CMMC requirements are adequately met. Provide actionable recommendations on how to remediate identified gaps.
- *CMMC Mock Assessment* – Perform a CMMC mock assessment to determine how well an organization would perform on an actual assessment.



For more information visit www.schneiderdowns.com/cmmc.

**SCHNEIDER DOWNS CMMC CONTACTS**

Eric M. Wright CPA, CITP – ewright@schneiderdowns.com

Troy Fine, CPA, CISSP, CISA – tfine@schneiderdowns.com

Sean Thomas, CISM, CISSP, MBA – sthomas@schneiderdowns.com

**ABOUT SCHNEIDER DOWNS IT RISK ADVISORY**

Schneider Downs' IT Risk Advisory practice helps certify that your organization is risk-focused, promotes sound IT controls, ensures the timely resolution of audit deficiencies, and informs management of the effectiveness of your risk management practices. Our dedicated professionals have experience working with a wide variety of industries and companies of all sizes. We will partner with you to provide comprehensive IT audits and compliance reviews that will ensure your organization has effective and efficient technology controls that better align the technology function with your business and risk strategies.

SCHNEIDER DOWNS

Big Thinking. Personal Focus.

www.schneiderdowns.com

**PITTSBURGH**
One PPG Place
Suite 1700
Pittsburgh, PA 15222
P 412.261.3644

**COLUMBUS**
65 E. State Street
Suite 2000
Columbus, OH 43215
P 614.621.4060

**WASHINGTON, D.C.**
1660 International Drive
Suite 600
McLean, VA 22102
P 571.380.9003