REGULATORY IMPACT ANALYSIS
Cybersecurity Maturity Model Certification (CMMC) 2.0
32 CFR part 170; RIN 0790-AL49

Background

The Department of Defense (DoD or Department) requires a secure and resilient supply chain to ensure the development, production, and sustainment of capabilities critical to national security. The DoD supply chain is targeted by adversaries with increasing frequency and sophistication, and to devastating effect. Therefore, implementation of cybersecurity standards and enforcement mechanisms are critically important. Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," emphasizes the need to strengthen cybersecurity protections for both the Federal Government and the private sector.

Nation-state adversaries attack the U.S. supply chain for a myriad of reasons, including exfiltration of valuable technical data (a form of industrial espionage); disruption to control systems used for critical infrastructure, manufacturing, and weapons systems; corruption of quality and assurance across a broad range of product types and categories; and manipulation of software to achieve unauthorized access to connected systems and to degrade the integrity of system operations. For example, since September 2020, major cyber-attacks such as the SolarWinds[1], Colonial Pipeline, Hafnium[2], and Kaseya[3] attacks, have been spearheaded by nation-state actors[4] and resulted in significant failures and disruption. In context of this threat, the size and complexity of defense procurement activities provide numerous pathways for adversaries to access DoD's sensitive systems and information. Moreover, adversaries continue to evolve their tactics, techniques, and procedures. For example, on April 28, 2022, CISA and the FBI issued an advisory on destructive "wiperware," a form of malware which can destroy valuable information [5]. Protection of DoD's sensitive unclassified information is critically important, and the DoD needs assurance that contactor information systems are adequately secured to protect such information when it resides on or transits those systems.

The Department is committed to working with defense contractors to protect DoD and the defense contractor sensitive unclassified information in accordance with requirements for Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

- Federal Contract Information (FCI): As defined in section 4.1901 of the Federal Acquisition Regulation (FAR), FCI means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public, such as that on public Web sites, or simple transactional information, such as that necessary to process payments.
- Controlled Unclassified Information (CUI): 32 CFR § 2002.4(h) defines CUI, in part, as 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, including FCI.

[1] https://www.gao.gov/assets/gao-22-104746.pdf
[2] https://www.ic3.gov/Media/News/2021/210310.pdf
[3] https://www.cisa.gov/uscert/ncas/current-activity/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa
[4] https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-26AUG2019.pdf
[5] https://www.cisa.gov/uscert/ncas/alerts/aa22-057a

In September 2020, the DoD published Defense Federal Acquisition Regulation Supplement (DFARS) interim rule (Case 2019-D041), which implemented DoD's initial vision for the Cybersecurity Maturity Model Certification (CMMC) Program ("CMMC 1.0") and outlined basic program features, to include: 5-level tiered model, CMMC Certified Third Party Assessment Organization (C3PAO) assessments in support of contractor and subcontractor certification, with no allowance for a Plan of Action and Milestones, and implementation of all security requirements by the time of a contract award. A total of 750 comments were received on the CMMC Program during the public comment period that ended on November 30, 2020. These comments highlighted a variety of industry concerns including concerns relating to the costs for a C3PAO certification, and the costs and burden associated with implementing, prior to award, the required process maturity and 20 additional cybersecurity practices that were included in CMMC 1.0. The Small Business Administration Office of Advocacy also raised similar concerns on the impact the rule would have on small businesses in the DIB.

Pursuant to DFARS clause 252.204-7012, DoD has required certain defense contractors and subcontractors to implement the security protections set forth in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Rev 2 to provide adequate security for sensitive unclassified DoD information that is processed, stored, or transmitted on contractor information systems and to document their implementation status, including any plans of action for any NIST SP 800-171 Rev 2 requirement not yet implemented, in a System Security Plan. The CMMC Program provides the Department the mechanism needed to verify that a defense contractor or subcontractor has implemented the security requirements at each CMMC Level and is maintaining that status across the contract period of performance, as required.

In calendar year (CY) 2021 DoD paused the planned CMMC rollout to conduct an internal review of the CMMC Program. The internal review resulted in a refined and streamlined set of requirements that addressed many of the concerns identified in the public comments received relating to CMMC 1.0. These changes have been incorporated into the CMMC Program structure and policies, now referred to as "CMMC 2.0." In July 2022, the CMMC PMO met with the Office of Advocacy for the United States Small Business Administration (SBA) to address the revisions planned in CMMC 2.0 that are responsive to prior SBA concerns.

The CMMC Program will enhance the ability of the DoD to safely share sensitive unclassified information with defense contractors and know the information will be suitably safeguarded. Once fully implemented, CMMC will incorporate a set of cybersecurity requirements into acquisition contracts to provide verification that applicable cyber protection standards have been implemented. Under the CMMC Program, defense contractors and subcontractors will be required to implement certain cybersecurity protection standards tied to a designated CMMC level and either perform a self-assessment or obtain an independent assessment from either a third-party or DoD as a condition of a DoD contract award. CMMC is designed to validate the protection of sensitive unclassified information that is shared with and generated by the Department's contractors and subcontractors. Through protection of information by adherence to the standards verified in CMMC 2.0, the Department and its contractors will prevent disruption in service and the loss of intellectual property and assets, and thwart access to sensitive unclassified information by the nation's adversaries.

The CMMC Program is intended to: (1) align cybersecurity requirements to the sensitivity of unclassified information to be protected, and (2) add a certification element, where appropriate, to verify implementation of cybersecurity requirements. As part of the program,

DoD also intends to provide supporting resources and training to the DIB to help support companies who are working to achieve the required CMMC level. The CMMC Program provides for assessment at three levels: basic safeguarding of Federal Contract Information (FCI) at CMMC Level 1, broad protection of CUI at CMMC Level 2, and enhanced protection of CUI against risk from Advanced Persistent Threats (APTs) at CMMC Level 3. The CMMC Program is designed to provide increased assurance to the Department that a defense contractor can adequately protect sensitive unclassified information (i.e., FCI and CUI) in accordance with prescribed security standards, accounting for information flow down to its subcontractors in a multi-tier supply chain.

The CMMC Program addresses DoD's need to protect its sensitive unclassified information during the acquisition and sustainment of products and services from the DIB. This effort is instrumental in establishing cybersecurity as a foundation for future DoD acquisition.

Although DoD contract requirements to provide adequate security for covered defense information (reflected in DFARS 252.204-7012) predate CMMC by many years, a certification requirement to assess a contractor or subcontractor's compliance of those required information security controls is new with the CMMC Program. Findings from DoD Inspector General report[6] indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take steps to assess a contractor's ability to protect this information. The report emphasizes that malicious actors can exploit the vulnerabilities of contractors' networks and systems and exfiltrate information related to some of the Nation's most valuable advanced defense technologies.

Currently, the FAR and DFARS prescribe contract clauses intended to protect FCI and CUI. Specifically, the clause at FAR 52.204–21, Basic Safeguarding of Covered Contractor Information Systems, is prescribed at FAR 4.1903 for use in Government solicitations and contracts when the contractor or a subcontractor at any tier may have FCI residing in or transiting through its information system(s). This clause requires contractors and subcontractors to implement basic safeguarding requirements and procedures to protect FCI being processed, stored, or transmitted on contractor information systems. In addition, DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is prescribed at DFARS 204.7304(c) for use in all solicitations and contracts except for solicitations and contracts solely for the acquisition of commercially available off-the-shelf (COTS) items. This clause requires contractors and subcontractors to provide "adequate security" to process, store or transmit covered defense information when it resides on or transits a contractor information system, and to report cyber incidents that affect that system or network. The clause states that to provide adequate security, the contractor shall implement, at a minimum, the security requirements in NIST Special Publication (SP) 800-171 Rev 2, Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations. Contractors are also required to flow down DFARS clause 252.204-7012 to all subcontracts that require processing, storing, or transmitting of covered defense information.

[6] DODIG-2019-105 "Audit of Protection of DoD CUI on Contractor-Owned Networks and Systems"

However, neither FAR clause 52.204-21 nor DFARS clause 252.204-7012 provide for DoD verification of a contractor's implementation of the basic safeguarding requirements specified in FAR 52.204-21 nor the security requirements specified in NIST SP 800-171 Rev 2, implementation of which is required by DFARS clause 252.204-7012, prior to contract award. As part of multiple lines of effort focused on the security and resilience of the DIB, the Department is working with industry to enhance the protection of FCI and CUI within the DoD supply chain. Toward this end, DoD has developed the CMMC Program.

CMMC 2.0 Requirements

The CMMC Program requirements will be implemented through the DoD acquisition and contracting process. With limited exceptions, the Department intends to require compliance with CMMC as a condition of contract award. Once CMMC is implemented, the required CMMC level for contractors will be specified in the solicitation. In accordance with the implementation plan described in 32 CFR § 170.3(e), CMMC compliance or certification requirements will apply to new DoD solicitations and contracts, and shall flow down to subcontractors, based on the sensitivity of the FCI and CUI to be processed, stored or transmitted to or by the subcontractor. Before contract award, the offeror must achieve the specified CMMC level for the contractor information system (e.g., enterprise network, network enclave) that will process, store, or transmit the information to be protected. The contractor or subcontractor will also submit affirmations in the Supplier Performance Risk System (SPRS). An overview of requirements at each level is shown below:

CMMC Level 1 Self-Assessment

- CMMC Level 1 Self-Assessment requires compliance with basic safeguarding requirements to protect Federal Contract Information (FCI) are set forth in FAR clause 52.204-21. CMMC Level 1 does not add any additional security requirements to those identified in FAR 52.204-21.
- Organizations Seeking Assessment (OSAs) will submit the following information in SPRS prior to award of any prime contract or subcontract and annually thereafter:
    1. the results of a self-assessment of the OSA's implementation of the basic safeguarding requirements set forth in 32 CFR § 170.15 associated with the contractor information system(s) used in performance of the contract; and
    2. an initial affirmation of compliance, and then annually thereafter, an affirmation of continued compliance as set forth in 32 CFR § 170.22.
- The Level 1 Self-Assessment cost burden will be addressed as part of the 48 CFR rule.

CMMC Level 2 Self-Assessment

- CMMC Level 2 Self-Assessment requires compliance with the security requirements set forth in NIST SP 800-171 Rev 2 to protect CUI. CMMC Level 2 does not add any additional security requirements to those identified in NIST SP 800-171 Rev 2.
- OSAs will submit the following information in SPRS prior to award of any prime contract or subcontract:
    1. the results of a self-assessment of the OSA's implementation of the NIST SP 800-171 Rev 2 requirements set forth in 32 CFR § 170.16 associated with the covered contractor

information system(s) used in performance of the applicable contract.

2. an initial affirmation of compliance, and, if applicable, a POA&M closeout affirmation, and then annually thereafter, an affirmation of continued compliance set forth in 32 CFR § 170.22.

- The Level 2 Self-Assessment cost burden will be addressed as part of the 48 CFR rule.

CMMC Level 2 Certification

- CMMC Level 2 Certification requires compliance with the security requirements set forth in in 32 CFR § 170.17 to protect CUI. CMMC Level 2 does not add any additional security requirements to those identified in NIST SP 800-171 Rev 2.
- A CMMC Level 2 Certification Assessment of the applicable contractor information system(s) provided by an authorized or accredited C3PAO is required to validate implementation of the NIST SP 800-171 Rev 2 security requirements prior to award of any prime contract or subcontract and exercise of option.
- The C3PAO will upload the CMMC Level 2 results in eMASS which will feed the information into SPRS.
- OSCs will submit in SPRS an initial affirmation of compliance, and, if necessary, a POA&M closeout affirmation, and then annually thereafter, an affirmation of continued compliance as set forth in 32 CFR § 170.22.
- The Level 2 Certification Assessment cost burdens are included in this 32 CFR rule with the exception of the requirement for the OSC to upload the affirmation in SPRS. Additionally, the eMASS information collection requirements only cover only those requirements pertaining to the CMMC process.

CMMC Level 3 Certification

- CMMC Level 3 Certification Assessment requires a CMMC Level 2 Final Certification Assessment and compliance with the security requirements set forth in 32 CFR § 170.18 to protect CUI. CMMC Level 3 adds additional security requirements to those required by existing acquisition regulations as specified in this rule.
- A CMMC Level 3 Certification Assessment of the applicable contractor information system(s) provided by the DCMA Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) is required to validate implementation of the DoD-defined selected security requirements set forth in NIST SP 800-172. A CMMC Level 2 Final Certification is a prerequisite to schedule a DIBCAC assessment for CMMC Level 3.
- DCMA DIBCAC will upload the CMMC Level 3 results in eMASS, which will feed the information into SPRS.
- OSCs will submit in SPRS an initial affirmation of compliance, and, if necessary, a POA&M closeout affirmation, and then annually thereafter, an affirmation of continued compliance as set forth in 32 CFR § 170.22.
- The Level 3 Certification Assessment cost burdens are included in this 32 CFR rule with the exception of the requirement for the OSC to upload the affirmation in SPRS. Additionally,

the eMASS information collection requirements only cover only those requirements pertaining to the CMMC process.

As described above, the CMMC Program couples an affirmation of compliance with certification assessment requirements to verify OSA implementation of cybersecurity requirements, as applicable.

The CMMC Program addresses DoD's need to protect its sensitive unclassified information during the acquisition and sustainment of products and services from the DIB. This effort is instrumental in ensuring cybersecurity is the foundation of future DoD acquisitions.

Policy Problems Addressed by CMMC 2.0

Implementation of the CMMC Program is intended to solve the following policy problems:

Verifies the Contractor Cybersecurity Requirements

Neither FAR clause 52.204-21 nor DFARS clause 252.204-7012 provide for DoD assessment of a defense contractor or subcontractor's implementation of the information protection requirements within those clauses. Defense contractors represent that they will implement the requirements in NIST SP 800-171 Rev 2 upon submission of their offer. Findings from DoD Inspector General report (DODIG-2019-105 "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems") indicate that DoD contractors did not consistently implement mandated system security requirements for safeguarding CUI and recommended that DoD take steps to assess a contractor's ability to protect this information. CMMC adds new requirements for the assessment of contractor implementation of underlying information security standards, to allow DoD to assess a defense contractor's cybersecurity posture using authorized or accredited C3PAOs. The contractor and subcontractor must achieve the required CMMC Level as a condition of contract award.

Implementation of Cybersecurity Requirements

Under DFARS clause 252.204-7012, defense contractors and subcontractors must document implementation of the security requirements in NIST SP 800-171 Rev 2 in a system security plan and may use a Plan of Action Milestones to describe how and when any unimplemented security requirements will be met. For the CMMC Program, the solicitation, will specify the required CMMC level, which will be determined considering program criticality, information sensitivity, and severity of cyber threat. Although the security requirements in NIST SP 800-171 Rev 2 address a range of threats, additional requirements are needed to significantly reduce the risk posed by APTs. An APT is an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). CMMC Level 3 requires implementation of selected security requirements from NIST SP 800-172 to reduce the risk of APT threats.

The CMMC Program will require prime contractors to flow the appropriate CMMC requirement down throughout the entire supply chain relevant to a particular contract. Defense contractors or subcontractors that handle FCI, must meet the requirements for CMMC Level 1. Defense contractors that handle CUI must meet the requirements for CMMC Level 2 or higher, depending on the sensitivity of the information associated with a program or technology being developed.

Scale and Depth

Today, DoD prime contractors must include DFARS clause 252.204-7012 in subcontracts for which performance will involve covered defense information, but this does not provide the Department with sufficient insights with respect to the cybersecurity posture of all members of a multi-tier supply chain for any given program or technology development effort. CMMC 2.0 requires prime contractors to flow down appropriate CMMC Level requirements, as applicable, to subcontractors throughout their supply chain(s).

Given the size and scale of the DIB, the Department cannot scale its existing cybersecurity assessment capability to conduct on-site assessments of approximately 220,000 DoD contractors and subcontractors every three years. The Department's existing assessment capability is best suited for conducting targeted assessments for the relatively small subset of DoD contractors and subcontractors that support designated high-priority programs involving CUI.

CMMC addresses the Department's scaling challenges by utilizing a private-sector accreditation structure. A DoD-authorized Accreditation Body will authorize, accredit, and provide oversight of C3PAOs which in turn will conduct CMMC Level 2 Certification Assessments of actual and prospective DoD contractors and subcontractors. Defense contractors will directly contract with an authorized or accredited C3PAO to obtain a CMMC Certification Assessment. The cost of CMMC Level 2 activities is driven by multiple factors, including market forces that govern availability of C3PAOs and the size and complexity of the enterprise or enclave under assessment. The Government will perform CMMC Level 3 Certification Assessments. Government resource limitations may affect schedule availability.

Reduces Duplicate or Respective Assessments of Our Industry Partners

CMMC assessment results will be posted in SPRS, DoD's authoritative source for supplier and product performance information. Posting CMMC assessment results in SPRS precludes the need to validate CMMC implementation on a contract-by-contract basis. This enables DoD to identify whether the CMMC requirements have been met for relevant contractor information systems, avoids duplicative assessments, and eliminates the need for program level assessments, all of which decreases costs to both DoD and industry.

CMMC 2.0 Implementation

The DoD is implementing a phased implementation for CMMC 2.0 and intends to introduce CMMC requirements in solicitations over a three-year period to provide appropriate ramp-up time. This phased implementation is intended to minimize the financial impacts to defense contractors, especially small businesses, and disruption to the existing DoD supply chain. After CMMC is implemented in acquisition regulation, DoD will include CMMC self-assessment requirements in solicitations when warranted by the type of information that will be handled by the contractor of subcontractor(s). CMMC requirements for Levels 1, 2, and 3 will be included in solicitations issued after the phase-in period when warranted by any FCI and/or CUI information protection requirements for the contract effort. In the intervening period, Government Program Managers will have discretion to include CMMC requirements or exclude them and rely upon existing DFARS Clause 252.204-7012 requirements, in accordance with DoD policy. As stated in 32 CFR §170.20(a), there is qualified standards acceptance between DCMA DIBCAC High NIST SP 800-171 Rev 2 DoD Assessment and CMMC Level 2, which

will result in staggering of the dates for new CMMC Level 2 assessments. The implementation period will consist of four (4) phases as set forth in 32 CFR § 170.3(e), during which time the Government will include CMMC requirements in certain solicitations and contracts. During the CMMC phase-in period, program managers and requiring activities will be required to include CMMC requirements in certain solicitations and contracts and will have discretion to include in others.

A purpose of the phased implementation is to ensure adequate availability of authorized or accredited C3PAOs and assessors to meet the demand.

CMMC 2.0 Flow Down

CMMC Level requirements will be flowed down to subcontractors at all tiers as set forth in 32 CFR § 170.23; however, the specific CMMC Level required for a subcontractor will be based on the type of unclassified information and the priority of the acquisition program and/or technology being developed.

Key Changes Incorporated in the CMMC 2.0 Program

In November 2021, the Department announced "CMMC 2.0," which is an updated program structure with revised requirements. In CMMC 2.0, the Department has introduced several key changes that build on and refine the original program requirements. These include:

- Streamlining the model from five levels to three levels.
- Exclusively implementing National Institute of Standards and Technology (NIST) cybersecurity standards.
- Allowing all companies subject to Level 1, and a subset of companies subject to Level 2 to demonstrate compliance through self-assessments.
- Increased oversight of professional and ethical standards of CMMC third-party assessors.
- Allowing Plans of Action & Milestones (POA&M) under limited circumstances to achieve conditional certification.

As a result of the alignment of CMMC 2.0 to NIST guidelines, the Department's requirements will continue to evolve as changes are made to the underlying NIST SP 800-171 Rev 2 and NIST SP 800-172 requirements.

CMMC Assessment

Assessment Criteria

CMMC requires that defense contractors and subcontractors entrusted with FCI and CUI implement cybersecurity standards at progressively more secure levels, depending on the type and sensitivity of the information.

CMMC Level 1 Self-Assessment

An annual CMMC Level 1 Self-Assessment and annual affirmation asserts that an OSA has implemented all the Basic Safeguarding requirements to protect FCI as set forth in 32 CFR § 170.14(c)(2).

An OSA can choose to perform the annual self-assessment internally or engage a third-party to assist with evaluating its Level 1 compliance. Use of a third party to assist with the assessment process is still considered a self-assessment and does not result in a CMMC certification. An OSA can be compliant with CMMC Level 1 requirements for an entire enterprise network or for a particular enclave(s), depending upon where the FCI is or will be processed, stored, or transmitted.

CMMC Level 2 Self-Assessment

A CMMC Level 2 Self-Assessment and triennial affirmation attests that an OSA has implemented all the security requirements to protect CUI as specified in 32 CFR § 170.14(c)(3).

CMMC Level 2 Certification Assessment

A CMMC Level 2 Certification Assessment, conducted by a C3PAO, verifies that an OSC is conforming to the security requirements to protect CUI as specified in 32 CFR § 170.14(c)(3). A CMMC Level 2 assessment must be conducted for each OSC information system that will be used in the execution of the contract that will process, store, or transmit CUI.

CMMC Level 3 Certification Assessment

Receipt of a CMMC Level 2 Final Certification Assessment for information systems within the Level 3 CMMC Assessment Scope is a prerequisite for a CMMC Level 3 Certification Assessment. A CMMC Level 3 Certification Assessment, conducted by DCMA Defense Industrial Base Cybersecurity Assessment Center (DIBCAC), verifies that an OSC has implemented the CMMC Level 3 security requirements to protect CUI as specified in 32 CFR § 170.14(c)(4). A CMMC Level 3 Certification Assessment must be conducted for each OSC information system that will be used in the execution of the contract that will process, store, or transmit CUI.

Impact and Cost Analysis of CMMC 2.0

Summary of Impact

Public comment feedback on CMMC 1.0 indicated that cost estimates were too low. CMMC 2.0 cost estimates account for that feedback with the following improvements:

- Allowance for outsourced IT services
- Increased total time for the contractor to prepare for the assessment, including limited time for learning the reporting and affirmation processes
- Allowance for use of consulting firms to assist with the assessment process
- Time for a senior level manager to review the assessment and affirmation before submitting the results in SPRS
- Updated government and contractor labor rates that include applicable burden costs

As a result, some CMMC 2.0 costs may be higher than those included in CMMC 1.0.

The CMMC 2.0 impact analysis includes estimated costs for implementation of CMMC 2.0 requirements across Level 1, Level 2, and Level 3 for the Public (small and other than small entities, including the CMMC Ecosystem as set forth in 32 CFR Subpart C) and the Government. In summary, the total estimated Public and Government costs associated with this rule, calculated over 20-year horizon in 2023 dollars at a 7 percent discount rate and a 3 percent discount rate are provided as follows:

Total Estimated Costs of CMMC Requirements for the Public and the Government (7 percent discount)			
Total cost	**Public**	**Government**	**Total**
Annualized Costs	$3,989,182,374	$9,508,593	$3,998,690,967
Present Value Costs	$42,261,454,899	$100,734,168	$42,362,189,067

Total Estimated Costs of CMMC Requirements for the Public and the Government (3 percent discount)			
Total cost	**Public**	**Government**	**Total**
Annualized Costs	$4,219,513,555	$9,953,205	$4,229,466,760
Present Value Costs	$62,775,706,830	$148,078,564	$62,923,785,394

The details that comprise the Public and Government costs by level are provided below.

In this cost analysis, each cost factor is illustrated over a ten-year period merely to identify the cost pattern behavior after year 7; however, the total annualized Public and Government costs associated with implementation of the CMMC Program is based on a 20-year time horizon.

Estimating the timing of CMMC assessment needs for unique entities per level per year is complicated by the fact that companies may serve as a prime contractor on one effort but a subcontractor on others, and may also enter into subcontract agreements with more than one prime contractor for various opportunities.

In addition, the CMMC Program relies upon free market influences of supply and demand to propel implementation. Specifically, the Department does not control which defense contractors aspire to compete for which business opportunities, nor does it control access to the assessment services offered by C3PAOs. OSAs may elect to complete a self-assessment or pursue a certification assessment at any time after issuance of the rule, in an effort to distinguish themselves as competitive for efforts that require an ability to adequately protect CUI. For that reason, the number of CMMC assessments for unique entities per level per year may vary significantly from the assumptions used in generating the cost estimate. The estimates represent the best estimates at this time based on internal expertise and public feedback.

DoD utilized historical metrics gathered for the CMMC 1.0 Program and subject matter expertise from Defense Pricing and Contracting (DPC) and DCMA DIBCAC to estimate the

number of entities by type and by assessment level for this analysis. The following table summarizes the estimated profile used in this analysis.

Estimated Number of Entities by Type and Level				
Assessment Level	**Small**	**Other than Small**	**Total**	**Percent**
Level 1 Self-Assessment	103,010	36,191	139,201	63%
Level 2 Self-Assessment	2,961	1,039	4,000	2%
Level 2 Certification Assessment	56,689	19,909	76,598	35%
Level 3 Certification Assessment	1,327	160	1,487	1%
Total	**163,987**	**57,299**	**221,286**	100%
Percent	74%	26%	100%	

DoD is planning for a phased roll-out of each assessment level across 7 years with the entity numbers reaching a maximum by Year 4 as shown in the tables below. The target of Year 4 was selected based on the projected capacity of the CMMC Ecosystem to grow to efficiently support the entities in the pipeline. For modeling efficiency, a similar roll-out is assumed regardless of entity size or assessment level. It is assumed that by year 7 the maximum number of entities is reached. Beyond year 7, the number of entities entering and exiting are expected to net to zero. The following tables reflect the number of new entities in each year and for each level.

*Number of Small Entities Over Phase-In Period					
	Level 1	**Level 2**	**Level 2**	**Level 3**	
Yr	**Self-Assess**	**Self-Assess**	**Certification**	**Certification**	**Total**
1	699	20	382	3	1,104
2	3,493	101	1,926	45	5,565
3	11,654	335	6,414	151	18,554
4	22,336	642	12,293	289	35,560
5	22,333	642	12,289	289	35,553
6	22,333	642	12,289	289	35,553
7	20,162	579	11,096	261	32,098
Tot	**103,010**	**2,961**	**56,689**	**1,327**	**163,987**

*Number of Other than Small Entities Over Phase-In Period					
	Level 1	**Level 2**	**Level 2**	**Level 3**	
Yr	**Self-Assess**	**Self-Assess**	**Certification**	**Certification**	**Total**
1	246	7	135	1	389
2	1,227	35	673	5	1,940
3	4,094	118	2,252	18	6,482
4	7,848	225	4,317	34	12,424
5	7,846	225	4,317	34	12,422

6	7,846	225	4,317	34	12,422
7	7,084	204	3,898	34	11,220
Tot	**36,191**	**1,039**	**19,909**	**160**	**57,299**

*Number of Total Entities Over Phase-In Period					
	Level 1	Level 2	Level 2	Level 3	
Yr	Self-Assess	Self-Assess	Certification	Certification	Total
1	945	27	517	4	1,493
2	4,720	136	2,599	50	7,505
3	15,748	453	8,666	169	25,036
4	30,184	867	16,610	323	47,984
5	30,179	867	16,606	323	47,975
6	30,179	867	16,606	323	47,975
7	27,246	783	14,994	295	43,318
Tot	**139,201**	**4,000**	**76,598**	**1,487**	**221,286**

Public Costs

Summary of Impact

According to data available in the Electronic Data Access system for fiscal years (FYs) 2019, 2020, and 2021, DoD awards an average of 1,366,262 contracts and orders per year that contain DFARS clause 252.204-7012, to 31,338 unique awardees, of which 683,718 awards (50%) are made to 23,475 small entities (75%).[7]

Public Cost Analysis

The following is a summary of the estimated Public costs CMMC 2.0 for other than small[8] entities, per assessment of a contractor information system, at the required periodicity for each CMMC level.

Table 1 - Other Than Small Entities (per Assessment)				
Assessment Phase ($)	**Level 1 Self-Assessment[9]**	**Level 2 Self-Assessment[9]**	**Level 2 Certification**	**Level 3 Certification**
Periodicity	Annual	Triennial	Triennial	Triennial
Plan and Prepare the Assessment	$1,146	$18,015	$26,264	$7,066
Conduct the Assessment	$1,728	$19,964	$80,656	$23,136

[7] The number of unique awardees impacted each year is 1/3 of the average number of annual awardees according to the Electronic Data Access system (31,338/3 = 10,446). This estimate does not address new entrants or awardees who discontinue doing business with DoD.

[8] Includes all businesses with the exception of those defined under the small business criteria and size standards provided in 13 CFR 121.201 (See FAR Part 19.102)

[9] The Level 1 and Level 2 Self-Assessment information collection reporting and recordkeeping requirements will be included in a modification of an existing DFARS collection approved under OMB Control Number 0750-0004, Assessing Contractor Implementation of Cybersecurity Requirements. Modifications to this DFARS collection will be addressed as part of the 48 CFR rule.

Report Assessment Results	$584	$2,712	$2,712	$2,712
Annual Affirmation(s)	$584	*$8,136	*$8,136	*$8,136
Subtotal	$4,042	$48,827	$117,768	$41,050
** POA&M	$0	$0	$0	$3,394
Total (across 3 years)	**$4,042**	**$48,827**	**$117,768**	**$44,444**

*Reflects the 3-year cost to match the periodicity.
**Requirements NOT MET (if needed and when allowed) will be documented in a Plan of Action and Milestones.

The following is a summary of the estimated Public costs CMMC 2.0 for Small Entities, per assessment of each contractor information system, estimated at one per entity, at the required periodicity for each CMMC level.

Table 2 - Small Entities (per Assessment)				
Assessment Phase ($)	**Level 1 Self-Assessment[10]**	**Level 2 Self-Assessment[10]**	**Level 2 Certification Assessment**	**Level 3 Certification Assessment**
Periodicity	Annual	Triennial	Triennial	Triennial
Plan and Prepare the Assessment	$1,803	$14,426	$20,699	$1,905
Conduct the Assessment	$2,705	$15,542	$76,743	$1,524
Report Assessment Results	$909	$2,851	$2,851	$1,876
Affirmations	$560	*$4,377	*$4,377	*$5,628
Subtotal	$5,977	$37,196	$104,670	$10,933
**POA&M	$0	$0	$0	$1,869
Total	**$5,977**	**$37,196**	**$104,670**	**$12,802**

*Reflects the 3-year cost to match the periodicity.
**Requirements "NOT MET" (if needed and when allowed) will be documented in a Plan of Action and Milestones.

The total estimated Public (large and small entities) costs associated with this rule, calculated for a 20-year horizon in 2023 dollars at a 7 percent and 3 percent discount rate,[11] per OMB guidance, is provided as follows:

Total Estimated Costs of CMMC Requirements for Large and Small Entities		
Public Costs	**7% Discount**	**3% Discount**
Annualized Costs	$3,989,182,374	$4,219,513,555
Present Value Costs	$42,261,454,899	$62,775,706,830

Assumptions

[10] The Level 1 and Level 2 Self-Assessment information collection reporting and recordkeeping requirements will be included in a modification of an existing DFARS collection approved under OMB Control Number 0750-0004, Assessing Contractor Implementation of Cybersecurity Requirements. Modifications to this DFARS collection will be addressed as part of the 48 CFR rule.
[11] The Office of Management and Budget (OMB) advises federal agencies to use the discount rates of 7 percent and 3 percent for policy costs analysis.

In estimating the Public costs, DoD considered applicable nonrecurring engineering costs, recurring engineering costs[12], assessment costs, and affirmation costs for each CMMC Level. For CMMC Levels 1 and 2, the cost estimates are based only upon the assessment, certification, and affirmation activities that a defense contractor, subcontractor, or ecosystem member must take to allow DoD to verify implementation of the relevant underlying security requirements, i.e., for CMMC Level 1, the security requirements set forth in FAR clause 52.204-21, and for CMMC Level 2, the security requirements set forth in NIST SP 800-171 Rev 2. DoD did not consider the cost of implementing the security requirements themselves because implementation is already required by FAR clause 52.204-21, effective June 15, 2016, and by DFARS clause 252.204-7012, requiring implementation by Dec. 31, 2017, respectively; therefore, the costs of implementing the security requirements for CMMC Levels 1 and 2 should already have been incurred and are not attributed to this rule. As such, the nonrecurring engineering and recurring engineering costs to implement the security requirements defined for CMMC Level 1 and Level 2 are not included in this economic analysis. However, cost estimates to implement CMMC Level 3, are included, as that CMMC level will require defense contractors and subcontractors, as applicable, to implement a DoD-defined subset of the security requirements set forth in NIST SP 800-172, a new addition to current security protection requirements.

In estimating the public cost for a defense contractor small entity to comply with CMMC Program requirements for each CMMC level, DoD considered non-recurring engineering costs, recurring engineering costs, assessment costs, and affirmation costs for each CMMC Level. These costs include labor and consulting.

Estimates include size and complexity assumptions to account for typical organizational differences between small entities and other than small entities with respect to the handling of Information Technology (IT) and cybersecurity:

- small entities are likely to have a less complex, less expansive operating environment and IT / Cybersecurity infrastructure compared to larger defense contractors
- small entities are likely to outsource IT and cybersecurity to an External Service Provider (ESP)
- entities (small and other than small) pursuing CMMC Level 2 Self-Assessment are likely to seek consulting or implementation assistance from an ESP to either help them prepare for the assessment technically or participate in the assessment with the C3PAOs.

Estimates do not include the cost to implement (Non-recurring Engineering Costs (NRE)) or maintenance costs (Recurring Engineering (RE)) the security requirements prescribed in current regulations.

For CMMC Levels 1 and 2, cost estimates are based upon assessment, reporting and affirmation activities that a contractor or subcontractor will need to take to verify implementation of existing cybersecurity requirements set forth in FAR clause 52.204-21, effective June 15, 2016, to protect FCI, and DFARS clause 252.204-7012 which required implementation of NIST SP 800-171 Rev 2 not later than December 31, 2017, to protect CUI. As such, cost estimates are not included for an entity to implement the CMMC Level 1 or 2 security requirements, maintain

[12] The terms nonrecurring engineering costs and recurring engineering costs are terms of art and do not only encompass actual engineering costs.

implementation of these existing security requirements, or remediate a Plan of Action for unimplemented requirements.

For CMMC Level 3, the cost estimates factor in the assessment, reporting, and affirmation activities in addition to estimates for NRE and RE to implement and maintain CMMC Level 3 security requirements. In addition to implementing the CMMC Level 2 security requirements, CMMC Level 3 requires implementing selected security requirement set forth in NIST SP 800-172 as described in 32 CFR § 170.14(c)(4) which are not currently required through other regulations. CMMC Level 3 is expected to apply only to a small subset of defense contractors and subcontractors.

The Cost Categories used for each CMMC Level are described below:

1. ***Nonrecurring Engineering Costs:*** Estimates consist of hardware, software, and the associated labor to implement the same. Costs associated with implementing the requirements set forth in FAR 52.204-21 and NIST SP 800-171 Rev 2 are assumed to have been already implemented and, therefore, are not accounted for in this cost estimate. As such, these costs only appear in CMMC Level 3. If nonrecurring engineering costs are referenced, they are only accounted for as a one-time occurrence and are reflected in the year of the initial assessment.
2. ***Recurring Engineering Costs:*** Estimates consist of annually recurring fees and associated labor for technology refresh. Costs associated with implementing the requirements set forth in FAR 52.204-21 and NIST SP 800-171 Rev 2 are assumed to have been already implemented and, therefore, are not accounted for in this cost estimate. As such, these costs only appear in CMMC Level 3.
3. ***Assessment Costs****:* Estimates consist of activities for pre-assessment preparations (which includes gathering and/or developing evidence that the assessment objectives for each requirement have been satisfied), conducting and/or participating in the actual assessment, and completion of any post-assessment work. Assessment costs are represented by notional phases. Assessment costs assume the OSA passes the assessment on the first attempt (conditional – with an allowable POA&M or final). Each phase includes an estimate of hours to conduct the assessment activities including:
    a) Labor hour estimates for a company (and any ESP support) to prepare for and participate in the assessment.
    b) C3PAO cost estimates for companies pursuing a certification
        - labor hour estimates for authorized or certified assessors to work with the business to conduct the actual assessment
        - Assessment Costs broken down into phases
        - Phase 1: *Planning and preparing for the assessment*
        - Phase 2: *Conducting the assessment* (self or C3PAO)
        - Phase 3: *Reporting of Assessment Results*
        - Phase 4: *POA&M Closeout* (for CMMC Level 3 only, if applicable and allowed)
            - CMMC allows a limited open Plan of Action and Milestones (POA&M) for a period of 180 days to remediate the POA&M, see 32 CFR § 170.21.
4. ***Affirmations:*** Estimates consist of costs for an OSA to submit to SPRS an initial and, as applicable, any subsequent affirmations of compliance that the contractor information

system is compliant with and will maintain compliance with the security requirements of the applicable CMMC Level. If POA&Ms are allowed, an affirmation must be submitted with the POA&M closeout. With the exception of Small Entities for Level 1 and Level 2, it is assumed the task requires the same labor categories and estimated hours as the final reporting phase of the assessment.

The categories and rates used for estimating purposes were compiled by subject matter experts based on current data available from within the DoD contractor database for comparable labor categories. A factor estimate of 30 percent was added to the labor rate per hour to include but are not limited to company-sponsored benefits (fringe) and limited employee-related expenses such as training and certifications. This estimate is based on labor performed by indirect personnel (i.e., personnel who are part of overhead expense); therefore, the 30 percent factor represents an estimate for fringe expense and G&A expenses versus full overhead expense. The categories and rates inclusive of the labor cost plus the additional factor are defined in the table below.

Other than Small Entities - Labor Rates Used for Estimate				
Code[13]	**Rate per Hour[14]**	**Description**	**Background / Years' Experience[15]**	**With Master's Degree[15]**
IT5	$ 116.87	Senior Staff IT Specialist	Cyber Background, 10 + years	
IT4	$ 97.49	Staff IT Specialist	Cyber Background, 7-10 years	5-7 years
IT3	$ 81.96	Senior IT Specialist	Cyber Background, 5-7 years	2-5 years
IT2	$ 54.27	IT Specialist	Cyber Background, 2-5 years	0-2 years
IT1	$ 36.32	Associate IT Specialist	Cyber Background, 0-2 years	
MGMT5	$ 190.52	Director	Chief Info. Systems Officer/ Chief Info. Officer	
MGMT4	$ 143.50	Staff Manager	Vice President	
MGMT3	$ 128.64	Senior Manager	Program Manager	
MGMT2	$ 95.96	Manager	5-7 years	
MGMT1	$ 82.75	Associate Manager	1-5 years	
C3PAO[16]	$ 260.28	Cyber Subject Matter Expert	4 years	

Small Entities - Labor Rates Used for Estimate				
Code[13]	**Rate per Hour[14]**	**Description**	**Background / Years' Experience[15]**	**With Master's Degree[15]**
MGMT5	$ 190.52	Director	Chief Info. Systems Officer / Chief Info. Officer	
IT4-SB	$ 86.24	Staff IT Specialist	Cyber Background, 7-10 years	5-7 years
ESP / C3PAO[16]	$ 260.28	Cyber Subject Matter Expert	4 years	

[13] IT = Information Technology, MGMT = Management
[14] IT and MGMT rates represent an estimate for in-house labor and includes the labor rate plus fringe expenses
[15] Background assumes a Bachelor's degree as the minimum education level, additional requirements are noted including required years of experience. A Master's degree may reduce the required years of experience as noted.
[16] The ESP / C3PAO rate represents an estimate for outsourced labor and includes the labor rate, overhead expense, G&A expense, and profit

CMMC Level 1 Self-Assessment and Affirmation Costs

Other Than Small Entities

- ***Nonrecurring and recurring engineering costs**:* There are no nonrecurring or recurring engineering costs associated with CMMC Level 1, since it is assumed that the contractor or subcontractor has already implemented the applicable security requirements.[17]
- ***Assessments Costs**:* It is estimated that the cost to support a CMMC Level 1 self-assessment and affirmation is ***$4,042** (as summarized in 4.1.2 above, Table 1). A Level I Self-Assessment is conducted annually, and is based on the assumptions detailed below:
  - **Phase 1: Planning and preparing for the assessment: $1,146**
    - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
    - A manager (MGMT2) for 4 hours ($95.96/hr x 4hrs = $384)
  - **Phase 2: Conducting the self-assessment**: **$1,728**
    - A director (MGMT5) for 6 hours ($190.52/hr x 6hrs = $1,143)
    - A staff IT specialist (IT4) for 6 hours ($97.49/hrs x 6hrs = $585)
  - **Phase 3: Reporting of assessment results** into SPRS: **$584**
    - A director (MGMT5) for 2 hours ($190.52/hr x 2hrs = $381)
    - A staff IT specialist (IT4) for 2.08 hours ($97.49/hrs x 2.08hrs = $203)
- **Affirmations**: It is estimated that the costs to perform an initial and annual affirmation of compliance with CMMC Level 1 for an "other than small" entity is **$584**
  - A director (MGMT5) for 2 hours ($190.52/hr x 2hrs = $381)
  - A staff IT specialist (IT4) for 2.08 hours ($97.49/hrs x 2.08hrs = $203)
- The Level 1 Self-Assessment and Affirmations cost burden will be addressed as part of the 48 CFR rule.
- **Summary**: The following is the annual other than small entities total cost summary for CMMC Level 1 self-assessments and affirmations over a ten-year period: (Example calculation, Year 1: ***$4,042** per entity (detailed above) x 246 entities (cumulative) = $994,233)

Year	Other than Small Entities Per Year	Cumulative Other Than Small Entities	Annual Total Cost (self-assess, affirm)
1	246	246	$994,233
2	1,227	1,473	$5,953,271
3	4,094	5,567	$22,499,565
4	7,848	13,415	$54,218,010
5	7,846	21,261	$85,928,372
6	7,846	29,107	$117,638,733
7	7,084	36,191	$146,269,399
8		36,191	$146,269,399
9		36,191	$146,269,399
10		36,191	$146,269,399
Total	**36,191**		**$872,309,779**

[17] CMMC Level 1 consists of the same 15 basic safeguarding requirements specified in FAR clause 52.204-21. This cost analysis assumes that DIB contractors and subcontractors already have contracts with FAR clause 52.204-21 and, therefore, have already implemented the 15 basic safeguarding requirements.

Small Entities

- ***Nonrecurring and recurring engineering costs***: There are no nonrecurring or recurring engineering costs associated with CMMC Level 1 since it is assumed the contractor or subcontractor has implemented the applicable security requirements.[18]
- ***Assessment Costs and Initial Affirmation Costs:*** It is estimated that the cost to support a CMMC Level 1 assessment and affirmation is ***$5,977** (as summarized in 4.1.2 above, Table 2). A Level I Self-Assessment is conducted annually, and is based on the assumptions detailed below:
  - **Phase 1: Planning and preparing for the assessment**: **$1,803**
    - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
    - An external service provider (ESP) for 4 hours ($260.28 x 4hrs = $1,041)
  - **Phase 2: Conducting the self-assessment**: **$2,705**
    - A director (MGMT5) for 6 hours ($190.52/hr x 6hrs = $1,143)
    - An external service provider (ESP) for 6 hours ($260.28 x 6hrs = $1,562)
  - **Phase 3: Reporting of assessment results** into SPRS: **$909**
    - A director (MGMT5) for 2 hours ($190.52/hr x 2hrs = $381)
    - An external service provider (ESP) for 2 hours ($260.28/hr * 2hrs = $521)
    - A staff IT specialist (IT4-SB) for 0.08 hours[19] ($86.24/hr x 0.08hrs = $7)
  - **Affirmation:** initial affirmation post assessment: **$ 560**
  - ***Reaffirmations****:* It is estimated that the costs to reaffirm a CMMC Level I annually for a small entity is **$560**
    - A director (MGMT5) for 2 hours ($190.52/hr x 2hrs = $381)
    - A staff IT specialist (IT4-SB) for 2.08 hours ($86.24/hr x 2.08hrs = $179)
  - The Level 1 Self-Assessment and Affirmations cost burden will be addressed as part of the 48 CFR rule.
- ***Summary****:* The following is the annual small entities total cost summary for CMMC Level 1 self-assessments and affirmations over a ten-year period: (Example calculation, Year 1: ***$5,977** per entity (detailed above) x 699 entities (cumulative) = $4,177,845)

Year	Small Entities Per Year	Cumulative Small Entities	Annual Total Cost (self-assess, affirm)
1	699	699	$4,177,845
2	3,493	4,192	$25,055,116
3	11,654	15,846	$94,709,771
4	22,336	38,182	$228,209,547
5	22,333	60,515	$361,691,392
6	22,333	82,848	$495,173,237
7	20,162	103,010	$615,679,258
8		103,010	$615,679,258
9		103,010	$615,679,258
10		103,010	$615,679,258
Total	**103,010**		**$3,671,733,942**

[18] Again, it is assumed that that DIB contractors and subcontractors have already implemented the 15 basic safeguarding requirements in FAR clause 52.204-21.

[19] A person needs to enter the information into SPRS, which should only take five minutes.

All Entities Summary:

The following is a summary of the combined costs for both small and other than small entities for CMMC Level 1 Self-Assessments and Affirmations over a ten-year period:

Year	Entities Per Year	Cumulative Entities	Total Cost (Self-Assess and Affirmation)
1	945	945	$5,172,077
2	4,720	5,665	$31,008,386
3	15,748	21,413	$117,209,336
4	30,184	51,597	$282,427,557
5	30,179	81,776	$447,619,764
6	30,179	111,955	$612,811,971
7	27,246	139,201	$761,948,657
8	0	139,201	$761,948,657
9	0	139,201	$761,948,657
10	0	139,201	$761,948,657
Total	**139,201**		**4,544,043,721**

CMMC Level 2 Self-Assessment and Affirmation Costs

Other Than Small Entities

- ***Nonrecurring and Recurring Engineering Costs****:* There are no nonrecurring or recurring engineering costs associated with CMMC Level 2 Self-Assessment since it is assumed the contractor or subcontractor has implemented the NIST SP 800-171 Rev 2 security requirements.
- ***Self-Assessment Costs and Initial Affirmation Costs****:* It is estimated that the cost to support a CMMC Level 2 self-assessment and affirmation is ***$43,403**. The three-year cost is $48,827 (as summarized in 4.1.2 above, Table 1), which includes the triennial assessment + affirmation, and two additional annual affirmations ($43,403 + $2,712 + $2,712).
  - **Phase 1: Planning and preparing for the assessment**: $**18,015**
    - A director (MGMT5) for 30 hours ($190.52/hr x 30hrs = $5,716)
    - A manager (MGMT2) for 40 hours ($95.96/hr x 40hrs = $3,838)
    - A staff IT specialist (IT4) for 46 hours ($97.49/hr x 46hrs = $4,485)
    - A senior IT specialist (IT3) for 26 hours ($81.96/hr x 26hrs = $2,131)
    - An IT specialist (IT2) for 34 hours ($54.27/hr x 34hrs = $1,845)
  - **Phase 2: Conducting the self-assessment**: **$19,964**
    - A director (MGMT5) for 24 hours ($190.52/hr x 24hrs = $4,572)
    - A manager (MGMT2) for 24 hours ($95.96/hr x 24hrs = $2,303)
    - A staff IT specialist (IT4) for 56 hours ($97.49/hr x 56hrs = $5,460)
    - A senior IT specialist (IT3) for 56 hours ($81.96/hr x 56hrs = $4,590)
    - An IT specialist (IT2) for 56 hours ($54.27/hr x 56hrs = $3,039)
  - **Phase 3: Reporting of Assessment Results** into SPRS: **$2,712**
    - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)

        - A manager (MGMT2) for 4 hours ($95.96/hr x 4hrs = $384)
        - A staff IT specialist (IT4) for 16 hours ($97.49/hr x 16hrs = $1,560)
        - A senior IT specialist (IT3) for 0.08 hours ($81.96/hr x 0.08hrs = $7)
    - **Affirmation**: initial affirmation post assessment: **$ 2,712**
- ***Reaffirmations****:* It is estimated that the cost to perform an annual affirmation for CMMC Level 2 Self-Assessment is **$2,712 (**three-year cost is $8,136, or $2,712 x 3)**:**
    - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
    - A manager (MGMT2) for 4 hours ($95.96/hr x 4hrs = $384)
    - A staff IT specialist (IT4) for 16 hours ($97.49/hr x 16hrs = $1,560)
    - A senior IT specialist (IT3) for 0.08 hours ($81.96/hr x 0.08hrs = $7)
- The Level 2 Self-Assessment and Affirmations cost burden will be addressed as part of the 48 CFR rule.
- ***Summary****:* The following is the annual other than small entities total cost summary for CMMC Level 2 Self-Assessments and Affirmations over a ten-year period: (Example calculation, Year 2: **(*$43,403** assessment per entity (detailed above) x 35 entities) + **($2,712** annual affirmation per entity x 7 entities) = $1,538,092

CMMC 2.0 Level 2: Self-Assessment for Other Than Small Entities			
Year	**Entities Performing Triennial Self-Assessments including initial affirmation**	**Entities Performing Annual Affirmation Actions Only**	**Total Cost**
1	7	0	$303,821
2	35	7	$1,538,092
3	118	42	$5,235,473
4	232	153	$10,484,485
5	260	350	$12,234,099
6	343	492	$16,221,701
7	436	603	$20,559,249
8	260	779	$13,397,691
9	343	696	$16,775,017
10	436	603	$20,559,249
Total	**2,470**	**3,725**	**$117,308,877**

Small Entities

- ***Nonrecurring and recurring engineering costs****:* There are no nonrecurring or recurring engineering costs associated with CMMC Level 2 Self-Assessment since it is assumed the contractor or subcontractor has implemented the NIST SP 800-171 Rev 2 security requirements.
- ***Self-Assessment Costs and Initial Affirmation Costs****:* It is estimated that the cost to support a CMMC Level 2 self-assessment and affirmation for a small entity is ***$34,277**. The three-year cost is $37,196 (as summarized in 4.1.2 above, Table 2), which includes the triennial assessment + affirmation, plus two additional annual affirmations ($34,277 + $1,459 + $1,459).

- **Phase 1**: **Planning and preparing for the assessment**: **$14,426**
  - A director (MGMT5) for 32 hours ($190.52/hr x* 32hrs = $6,097)
  - An external service provider (ESP) for 32 hours ($260.28/hr x 32hrs = $8,329)
- **Phase 2: Conducting the self-assessment: $15,542**
  - A director (MGMT5) for 16 hours ($190.52/hr x 16hrs = $3,048)
  - An external service provider (ESP) for 48 hours ($260.28/hr x 48hrs = $12,493)
- **Phase 3**: **Reporting of Assessment Results** into SPRS: **$2,851**
  - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
  - An external service provider (ESP) for 8 hours ($260.28/hr x 8hrs = $2,082)
  - A staff IT specialist (IT4-SB) for 0.08 hours ($86.24/hr x 0.08hrs = $7)
- **Affirmations**: initial affirmation post assessment: **$ 1,459**

- ***Reaffirmations:*** It is estimated that the costs to reaffirm a CMMC Level 2 Self-Assessment annually is **$1,459** (three-year costs to reaffirm a CMMC Level 2 Self-Assessment annually is $4,377, or $1,459 x 3):
  - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
  - A staff IT specialist (IT4-SB) for 8.08 hours ($86.24/hr x 8.08hrs = $697)
- The Level 2 Self-Assessment and Affirmations cost burden will be addressed as part of the 48 CFR rule.
- ***Summary****:* The following is the annual small entities total cost summary for CMMC Level 2 Self-Assessments and Affirmations over a ten-year period: (Example calculation, Year 2: **(*$34,277** self-assessment per entity x 101 entities) + (**$1,459** annual affirmation per entity x 20 entities) = $3,491,193)

CMMC 2.0 Level 2: Self-Assessment for Small Entities			
Year	**Entities Performing Triennial Self-Assessments including initial affirmation**	**Entities Performing Annual Affirmation Actions Only**	**Total Cost**
1	20	0	$685,547
2	101	20	$3,491,193
3	335	121	$11,659,448
4	662	436	$23,327,706
5	743	997	$26,922,622
6	977	1,405	$35,538,762
7	1,241	1,720	$45,047,546
8	743	2,218	$28,703,951
9	977	1,984	$36,383,471
10	1,241	1,720	$45,047,546
Total	**7,040**	**10,621**	**$256,807,792**

All Entities Summary

The following is a summary of the cost to all entities regardless of size for CMMC Level 2 Self-Assessments and affirmations over a ten-year period:

CMMC 2.0 Level 2: Self-Assessment for All Entities			
Year	**Entities Performing Triennial Self-Assessments and initial affirmation**	**Entities Performing Annual Reaffirmations Actions Only**	**Total Cost**
1	27	0	$989,369
2	136	27	$5,029,285
3	453	163	$16,894,921
4	894	589	$33,812,191
5	1,003	1,347	$39,156,721
6	1,320	1,897	$51,760,463
7	1,677	2,323	$65,606,795
8	1,003	2,997	$42,101,642
9	1,320	2,680	$53,158,488
10	1,677	2,323	$65,606,795
Total	**9,510**	**14,346**	**$374,116,669**

CMMC Level 2 Certification Assessment and Affirmation Costs

Other Than Small Entities

- ***Nonrecurring and recurring engineering costs****:* There are no nonrecurring or recurring engineering costs associated with CMMC Level 2 Certification Assessment since it is assumed the contractor or subcontractor has implemented the NIST SP 800-171 Rev 2 security requirements.
- ***Assessment and Initial Affirmation Costs****:* It is estimated that the cost to support a CMMC Level 2 Certification Assessment and annual affirmation for an "other than small" entity is ***$112,345**. The three-year cost is **$**117,768 (as summarized in 4.1.2 above, Table 1), and includes a triennial assessment + affirmation, plus two additional annual affirmations ($112,345 + $2,712 + $2,712, with a minor rounding difference.)
  - **Phase 1: Planning and preparing for the assessment**: **$26,264**
    - A director (MGMT5) for 32 hours ($190.52/hr x 32hrs = $6,097)
    - A manager (MGMT2) for 64 hours ($95.96/hr x 64hrs = $6,141)
    - A staff IT specialist (IT4) for 72 hours ($97.49/hr x 72hrs = $7,019)
    - A senior IT specialist (IT3) for 40 hours ($81.96/hr x 40hrs = $3,278)
    - An IT specialist (IT2) for 58 hours ($54.27/hr x 58hrs = $3,148)
    - An associate IT specialist (IT1) for 16 hours ($36.32/hr x 16hrs = $581)
  - **Phase 2: Conducting the assessment**: **$28,600**
    - A director (MGMT5) for 32 hours ($190.52/hr x 32hrs = $6,097)
    - A manager (MGMT2) for 32 hours ($95.96/hr x 32hrs = $3,071)
    - A staff IT specialist (IT4) for 72 hours ($97.49/hr x 72hrs = $7,019)

        - A senior IT specialist (IT3) for 72 hours ($81.96/hr x 72hrs = $5,901)
        - An IT specialist (IT2) for 120 hours ($54.27/hr x 120hrs = $6,512)
    - **Phase 3: Reporting of Assessment Results**: **$2,712**
        - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
        - A manager (MGMT2) for 4 hours ($95.96/hr x 4hrs = $384)
        - A staff IT specialist (IT4) for 16 hours ($97.49/hr x 16hrs = $1,560)
        - A senior IT specialist (IT3) for 0.08 hours ($81.96/hr x 0.08hrs = $7)
    - **Affirmation**: initial affirmation post assessment: **$2,712**
    - **C3PAO Costs:** C3PAO engagement inclusive of Phases 1, 2, and 3 (5-person team) for 200 hours ($260.28/hr x 200hrs = **$52,056**)
- ***Reaffirmations****:* It is estimated that the costs to reaffirm a CMMC Level 2 Certification Assessment annually is **$2,712** (three-year cost is $8,136 or $2,712 x 3)
    - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
    - A manager (MGMT2) for 4 hours ($95.96/hr x 4hrs = $384)
    - A staff IT specialist (IT4) for 8 hours ($97.49/hr x 8hrs = $1,560)
    - A senior IT specialist (IT3) for 0.08 hours ($81.96/hr x 0.08hrs = $7)
- The Level 2 Affirmations cost burden will be addressed as part of the 48 CFR rule.
- ***Summary****:* The following is the annual other than small entities total cost summary for CMMC Level 2 Certifications and Affirmations over a ten-year period: (Example calculation, Year 2: (***$112,345** assessment per entity (detailed above) x 673 entities) + (**$2,712** annual affirmation per entity x 135 entities) = $75,974,425)

CMMC 2.0 Level 2: Certification for Other Than Small Entities			
Year	**Entities Performing Triennial Certifications and initial affirmation**	**Entities Performing Annual Reaffirmation Actions Only**	**Total Cost**
1	135	0	$15,166,590
2	673	135	$75,974,425
3	2,252	808	$255,192,758
4	4,452	2,925	$508,094,016
5	4,990	6,704	$578,785,599
6	6,569	9,442	$763,604,903
7	8,350	11,559	$969,433,559
8	4,990	14,919	$601,067,429
9	6,569	13,340	$774,177,583
10	8,350	11,559	$969,433,559
Total	**47,330**	**71,391**	**$5,510,930,421**

Small Entities

- ***Nonrecurring or recurring engineering costs****:* There are no nonrecurring or recurring engineering costs associated with CMMC Level 2 Certification Assessment since it is assumed the contractor or subcontractor has implemented the NIST SP 800-171 Rev 2 security requirements.
- ***Assessment Costs and Initial Affirmation Costs****:* It is estimated that the cost to support a CMMC Level 2 Certification Assessment and affirmation for a small entity is ***$101,752.**

The three-year cost is $104,670 (as summarized in 4.1.2 above, Table 2), and includes the triennial assessment + affirmation plus two additional annual affirmations ($101,752 + $1,459 + $1,459).

- **Phase 1: Planning and preparing for the assessment**: **$20,699**
  - A director (MGMT5) for 54 hours ($190.52/hr x 54hrs = $10,288)
  - An external service provider (ESP) for 40 hours ($260.28/hr x 40hrs = $10,411)
- **Phase 2: Conducting the C3PAO-assessment**: **$45,509**
  - A director (MGMT5) for 64 hours ($190.52/hr x 64hrs = $12,193)
  - An external service provider (ESP) for 128 hours ($260.28/hr x 128hrs = $33,316)
- **Phase 3: Reporting of Assessment Results**: **$2,851**
  - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
  - An ESP for 8 hours ($260.28/hr x 8hrs = $2,082)
  - A staff IT specialist (IT4-SB) for 0.08 hours ($86.24/hr x 0.08hrs = $7)
- **Affirmations:** cost to post initial affirmation **$1,459**
- **C3PAO Costs:** C3PAO engagement inclusive of Phases 1, 2, and 3 (3-person team) for 120 hours ($260.28/hr x 120hrs = **$31,234**)

- ***Reaffirmations****:* It is estimated that the costs to reaffirm a CMMC Level 2 Certification Assessment annually is **$1,459** (three-year cost is $4,377, or $1,459 x 3)
  - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
  - A staff IT specialist (IT4-SB) for 8.08 hours ($86.24/hr x 8.08hrs = $697)
- The Level 2 Affirmations cost burden will be addressed as part of the 48 CFR rule.
- ***Summary****:* The following is the annual small entities total cost summary for CMMC Level 2 Certifications and Affirmations over a ten-year period: (Example calculation, Year 2: (***$101,752** assessment per entity x 1,926 entities) + (**$1,459** annual affirmation per entity x 382 entities) = $196,531,451)

CMMC 2.0 Level 2: Certification for Small Entities			
Year	**Entities Performing Triennial Certifications and initial affirmation**	**Entities Performing Annual Reaffirmation Actions Only**	**Total Cost**
1	382	0	$38,869,223
2	1,926	382	$196,531,451
3	6,414	2,308	$656,003,811
4	12,675	8,340	$1,301,872,564
5	14,215	19,089	$1,474,252,306
6	18,703	26,890	$1,942,295,763
7	23,771	32,918	$2,466,768,671
8	14,215	42,474	$1,508,368,920
9	18,703	37,986	$1,958,483,830
10	23,771	32,918	$2,466,768,671
Total	**134,775**	**203,305**	**$14,010,215,209**

All Entities Summary:

The following is a summary of the cost to all entities regardless of size for CMMC Level 2 Certification and Affirmation costs over a ten-year period:

CMMC 2.0 Level 2: Certification for All Entities			
Year	**Entities Performing Triennial Certifications and initial affirmation**	**Entities Performing Reaffirmation Actions Only**	**Total Cost**
1	517	0	$54,035,813
2	2,599	517	$272,505,876
3	8,666	3,116	$911,196,569
4	17,127	11,265	$1,809,966,579
5	19,205	25,793	$2,053,037,904
6	25,272	36,332	$2,705,900,665
7	32,121	44,477	$3,436,202,230
8	19,205	57,393	$2,109,436,349
9	25,272	51,326	$2,732,661,414
10	32,121	44,477	$3,436,202,230
Total	**182,105**	**274,696**	**$19,521,145,630**

CMMC Level 3 Certification Assessment and Affirmation Costs

An OSC pursuing Level 3 Certification must have a CMMC Level 2 Final Certification Assessment, and also must demonstrate compliance with CMMC Level 3, which includes implementation of selected security requirements from NIST SP 800-172 not required in prior rules. Therefore, the Nonrecurring Engineering and Recurring Engineering cost estimates have been included for the initial implementation and maintenance of the required selected NIST SP 800-172 requirements. The cost estimates below account for time for an OSC to implement these security requirements and prepare for, support, participate in, and closeout a CMMC Level 3 Certification Assessment conducted by DCMA DIBCAC. The OSC should keep in mind that the total cost of a CMMC Level 3 Certification Assessment includes the cost of a Level 2 Certification Assessment as well as the costs to implement and assess the security requirements specific to Level 3. CMMC Level 3 is expected to affect a small subset of the DIB.

Other Than Small Entities, Per Entity

- ***Nonrecurring Engineering Costs**:* **$21,100,000**[20]
- ***Recurring Engineering Costs**:* **$4,120,000**
- ***Assessment Costs and Initial Affirmation Costs**:* It is estimated that the cost to support a CMMC Level 3 Certification and affirmation for an other than small entity is ***$39,021.** The three-year cost is $44,445 (as summarized in 4.1.2 above, Table 1), and includes the triennial assessment + affirmation, plus two additional annual affirmations ($39,021 + $2,712 + $2,712)
  - **Phase 1**: **Planning and preparing for the assessment: $7,066**
    - A director (MGMT5) for 12 hours ($190.52/hr x 12hrs = $2,286)

[20] DoD utilized subject matter expertise from Defense Pricing and Contracting (DPC) and DCMA DIBCAC to estimate the Nonrecurring and Recurring Engineering Costs.

        - A manager (MGMT2) for 12 hours ($95.96/hr x 12hrs = $1,152)
        - A staff IT specialist (IT4) for 16 hours ($97.49/hr x 16hrs = $1,560)
        - A senior IT specialist (IT3) for 12 hours ($81.96/hr x 12hrs = $984)
        - An IT specialist (IT2) for 20 hours ($54.27/hr x 20hrs = $1,085)
    - **Phase 2: Conducting the assessment**: **$23,136**
        - A director (MGMT5) for 24 hours ($190.52/hr x 24hrs = $4,572)
        - A manager (MGMT2) for 24 hours ($95.96/hr x 24hrs = $2,303)
        - A staff IT specialist (IT4) for 64 hours ($97.49/hr x 64hrs = $6,239)
        - A senior IT specialist (IT3) for 64 hours ($81.96/hr x 64hrs = $5,245)
        - An IT specialist (IT2) for 88 hours ($54.27/hr x 88hrs = $4,776)
    - **Phase 3: Reporting of assessment results: $2,712**
        - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
        - A manager (MGMT2) for 4 hours ($95.96/hr x 4hrs = $384)
        - A staff IT specialist (IT4) for 16 hours ($97.49/hr x 16hrs = $1,560)
        - A senior IT specialist (IT3) for 0.08 hours ($81.96/hr x 0.08hrs = $7)
    - **Phase 4: Closing out POA&Ms[21] (for CMMC Level 3 if necessary and allowed**): $**3,394**
        - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
        - A senior staff IT specialist (IT5) for 16 hours ($116.87/hr x 16hrs = $1,870)
    - **Affirmations:** initial affirmation post assessment: **$2,712**
- ***Reaffirmations****:* It is estimated that the costs to reaffirm a CMMC Level 3 Certification Assessment annually is **$2,712** (three-year cost is $8,136, or $2,712 x 3)
    - A director (MGMT5) for 4 hours ($190.52/hr x 4hrs = $762)
    - A manager (MGMT2) for 4 hours ($95.96/hr x 4hrs = $384)
    - A staff IT specialist (IT4) for 16 hours ($97.49/hr x 16hrs = $1,560)
    - A senior IT specialist (IT3) for 0.08 hours ($81.96/hr x 0.08hrs = $7)

[21] Costs for closing out POA&Ms are included at Level 3 because the requirement to implement a subset of NIST SP 800-172 security requirements is new with the CMMC rule. These costs are not included at Level 2 because the implementation of all NIST SP 800-171 Rev 2 security requirements are already required.

- The Level 3 Affirmations cost burden will be addressed as part of the 48 CFR rule.
- ***Summary****:* The following is the annual other than small entities total cost summary for CMMC Level 3 Certifications and Affirmations over a ten-year period. Example calculation, Year 2 (reference per entity amounts shown above): **($39,021** Certification per entity x 5 entities) + (**$2,712** Annual Affirmation per entity x 1 entity) = $197,818, and
  - $105,500,000 Nonrecurring Engineering cost (**$21,100,000** per entity x 5 entities being certified), and
  - $24,720,000 Recurring Engineering cost (**$4,120,000** per entity x 5 entities being certified) + ($4,120,000 per entity x 1 entity performing affirmations)
  - $130,417,818 Total Cost = Certification and Affirmation Cost ($197,818) + Nonrecurring Engineering cost ($105,500,000) + Recurring Engineering cost ($24,720,000), or $145,432,897.

CMMC 2.0 Level 3 Certification for Other Than Small Entities						
Yr	**Entities Performing Triennial Certification Including Initial Affirmation**	**Entities Performing Re-affirmation Actions Only**	**Triennial Certification and Affirmations Total Cost**	**Nonrecurring Engineering Cost**	**Recurring Engineering Cost**	**Total Cost**
1	1	0	$39,021	$21,100,000	$4,120,000	$25,259,021
2	5	1	$197,818	$105,500,000	$24,720,000	$130,417,818
3	18	6	$718,654	$379,800,000	$98,880,000	$479,398,654
4	35	23	$1,428,123	$717,400,000	$238,960,000	$957,788,123
5	39	53	$1,665,578	$717,400,000	$379,040,000	$1,098,105,578
6	52	74	$2,229,811	$717,400,000	$519,120,000	$1,238,749,811
7	69	91	$2,939,280	$717,400,000	$659,200,000	$1,379,539,280
8	39	121	$1,850,016		$659,200,000	$661,050,016
9	52	108	$2,322,031		$659,200,000	$661,522,031
10	69	91	$2,939,280		$659,200,000	$662,139,280
Tot	**379**	**568**	**$16,329,613**	**$3,376,000,000**	**$3,901,640,000**	**$7,293,969,613**

Small Entities

- ***Nonrecurring Engineering Costs****:* **$2,700,000**
- ***Recurring Engineering Costs****:* **$490,000**
- ***Assessment Costs and Initial Affirmation Costs****:* It is estimated that the cost to support a CMMC Level 3 Certification Assessment for a small entity is ***$9,050** The three-year cost is $12,802 (summarized in 4.1.2 above, Table 2), and includes the triennial assessment + affirmation, plus two additional annual affirmations ($9,050 + $1,876 + $1,876):
  - **Phase 1: Planning and preparing for the assessment**: **$1,905**
    - A director (MGMT5) for 10 hours ($190.52/hr x 10hrs = $1,905)
  - **Phase 2: Conducting the assessment**: **$1,524**

        - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
    - **Phase 3: Reporting of Assessment Results**: **$1,876**
        - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
        - A staff IT specialist (IT4-SB) for 4.08 hours ($86.24/hr x 4.08hrs = $352)
    - **Phase 4: Closing out POA&Ms[22] (for CMMC Level 3 if necessary and allowed)**: **$1,869**
        - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
        - A staff IT specialist (IT4-SB) for 48 hours ($86.24/hr x 48hrs = $345)
- ***Reaffirmations**:* It is estimated that the costs to reaffirm a CMMC Level 3 Certification Assessment annually is **$1,876** (three-year cost is $5,628, or $1,876 x 3)
    - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
    - A staff IT specialist (IT4-SB) for 4.08 hours ($86.24/hr x 4.08hrs = $352)
- The Level 3 Affirmations cost burden will be addressed as part of the 48 CFR rule.
- ***Summary:*** The following is the annual small entities total cost summary for CMMC Level 3 Certifications and Affirmations over a ten-year period. Example calculation, Year 2 (reference per entity amounts above):
    - *($9,050 Certification per entity x 45 entities) + ($1,876 Annual Affirmation per entity x 3 entities) = $412,897, and
    - $121,500,000 Nonrecurring Engineering cost ($2,700,000 per entity x 45 entities being certified), and
    - $23,520,000 Recurring Engineering cost ($490,000 per entity x 45 entities being certified) + ($490,000 per entity x 3 entities performing affirmations)
    - $145,432,897 Total Cost = Certification and Affirmation Cost ($412,897) + Nonrecurring Engineering cost ($121,500,000) + Recurring Engineering cost ($23,520,000), or $145,432,897.

CMMC 2.0 Level 3 Certification for Small Entities						
Yr	**Entities Performing Triennial Certification Including Initial Affirmation**	**Entities Performing Re-affirmation Actions Only**	**Triennial Certification and Affirmations Total Cost**	**Nonrecurring Engineering Cost**	**Recurring Engineering Cost**	**Total Cost**
1	3	0	$27,151	$8,100,000	$1,470,000	$9,597,151
2	45	3	$412,897	$121,500,000	$23,520,000	$145,432,897
3	151	48	$1,456,663	$407,700,000	$97,510,000	$506,666,663
4	292	196	$3,010,423	$780,300,000	$239,120,000	$1,022,430,423
5	334	443	$3,853,914	$780,300,000	$380,730,000	$1,164,883,914
6	440	626	$5,156,569	$780,300,000	$522,340,000	$1,307,796,569
7	553	774	$6,456,917	$704,700,000	$650,230,000	$1,361,386,917
8	334	993	$4,885,718		$650,230,000	$655,115,718

[22] Costs for closing out POA&Ms are included at Level 3 because the requirement to implement a subset of NIST SP 800-172 security requirements is new with the CMMC rule. These costs are not included at Level 2 because the implementation of all NIST SP 800-171 Rev 2 security requirements are already required.

9	440	887	$5,646,207		$650,230,000	$655,876,207
10	553	774	$6,456,917		$650,230,000	$656,686,917
Tot	**3,145**	**4,744**	**$37,363,377**	**$3,582,900,000**	**$3,865,610,000**	**$7,485,873,377**

All Entities Summary

The following is a summary of the cost to all entities regardless of size for Level 3 CMMC Certification Assessments and affirmations over a ten-year period:

CMMC 2.0 Level 3 Certification for All Entities						
Yr	**Entities Performing Triennial Certification Including Initial Affirmation**	**Entities Performing Re-affirmation Actions Only**	**Triennial Certs and Affirmation Total Cost**	**Nonrecurring Engineering Cost**	**Recurring Engineering Cost**	**Total Cost**
1	4	0	$66,172	$29,200,000	$5,590,000	$34,856,172
2	50	4	$610,715	$227,000,000	$48,240,000	$275,850,715
3	169	54	$2,175,317	$787,500,000	$196,390,000	$986,065,317
4	327	219	$4,438,546	$1,497,700,000	$478,080,000	$1,980,218,546
5	373	496	$5,519,492	$1,497,700,000	$759,770,000	$2,262,989,492
6	492	700	$7,386,381	$1,497,700,000	$1,041,460,000	$2,546,546,381
7	622	865	$9,396,197	$1,422,100,000	$1,309,430,000	$2,740,926,197
8	373	1,114	$6,735,735	$-	$1,309,430,000	$1,316,165,735
9	492	995	$7,968,238	$-	$1,309,430,000	$1,317,398,238
10	622	865	$9,396,197	$-	$1,309,430,000	$1,318,826,197
Tot	**3,524**	**5,312**	**$53,692,990**	**$6,958,900,000**	**$7,767,250,000**	**$14,779,842,990**

Government Costs

Summary of Impact

The following is a summary of the estimated Government costs calculated over a 20-year horizon in 2023 dollars at a 7 percent and 3 percent discount rate. The Government costs include conducting Level 3 Certification Assessments, uploading results to CMMC eMASS, and the CMMC PMO costs.

Government Costs	7% Discount	3% Discount
Annualized Costs	$9,508,593	$9,953,205
Present Value Costs	$100,734,168	$148,078,564

Government Costs (All Levels)

The estimated Government costs utilize the entity numbers and phased roll-out detailed in the Public cost section above. The DIBCAC estimated the detailed hours for all activities and other costs in a manner similar to the details shown in the Public cost section above. Labor efforts for the Government are focused in Level 3. For purposes of the cost estimate, Government labor is based on the average of step one, five, and ten for GS-11 through GS-15 labor elements for the Washington D.C. area. The cost of labor was increased by a factor of approximately 51 percent which includes an estimated fringe factor (fringe factor includes estimated average insurance and pension benefits) plus overhead (overhead factor represents supervision and management of the labor) to arrive at the estimated labor rates. The Government labor in this estimate is performed by DCMA, which is a labor-intensive agency with limited overhead expenses. Therefore, the overall added factor of 51 percent is appropriate versus a typical full overhead factor of 100 percent.

CMMC Database Infrastructure Costs

The Government will develop the operational CMMC eMASS. The cost analysis assumes that the nonrecurring engineering (NRE) cost includes the requirements development, architecture design, security, prototyping and testing, and approvals or certifications.[23] Nonrecurring engineering costs is a one-time fee of **$4,631,213** and is reflected here as incurred in the initial year of the estimate. The Year 1 amount is based on the actual cost incurred in FY2020 with adjustment for inflation to arrive at base year (BY) 1 dollars (2023).

The recurring engineering (RE) cost includes database management, data analysis, cybersecurity, storage and backups, licensing, and infrastructure.[24]

The cost for recurring engineering in Year 1 **($2,336,038)** and Year 2 **($1,804,480)** are based on historical amounts incurred for FY 2020 and FY 2021 with adjustment for inflation to arrive at base year Year 1 and Year 2 dollars (2023 and 2024). The estimated recurring engineering for Year 3 forward is calculated as the average of the Year 1 and Year 2 amounts (($2,336,038 + $1,804,480)/2 = **$2,070,259**).

The table below summarizes the nonrecurring engineering (NRE) and recurring engineering (RE) costs for Year 1 through Year 5:

	Government Costs for CMMC Database Infrastructure (BY23$)		
	NRE	**RE**	**Sub-Total Per Year**
Year 1	$4,631,213	$2,336,038.92	$6,967,252
Year 2	0	$1,804,480	$1,804,480
Year 3	0	$2,070,259	$2,070,259
Year 4	0	$2,070,259	$2,070,259
Year 5	0	$2,070,259	$2,070,259

[23] Nonrecurring engineering costs were first incurred in FY20. The cost below has inflation applied to put the value in 2023 base year (BY) dollars.

[24] The cost for the recurring engineering cost below is based on the costs incurred in FY20 and FY21. The values for Year 1 (FY20) and Year 2 ((FY21) are actual historic values that have inflation applied to them to put them in base year 2023 dollars. Every proceeding years' recurring engineering cost is based on the average of the two historic actual values.

Total	**$4,631,213**	**$10,351,296**	**$14,982,509**

Total Government Costs

The following is a summary of the total Government costs over a ten-year period:

Year	Government Costs (All Levels**)	CMMC Database Infrastructure (CMMC eMASS)	Total
1	$79,698	$6,967,252	$7,046,950
2	$826,063	$1,804,480	$2,630,543
3	$2,871,167	$2,070,259	$4,941,426
4	$5,713,930	$2,070,259	$7,784,189
5	$6,830,268	$2,070,259	$8,900,527
6	$9,083,729	$2,070,259	$11,153,988
7	$11,533,002	$2,070,259	$13,603,261
8	$7,670,055	$2,070,259	$9,740,314
9	$9,486,082	$2,070,259	$11,556,342
10	$11,533,002	$2,070,259	$13,603,261

**Government activities associated with all Government costs associated with the CMMC Program.

Total Public and Government Costs

The following is a summary of the total estimated annual Public and Government cost associated with implementation of the CMMC Program over a ten-year period:

Estimated CMMC Costs – Public and Government (BY23$[25])			
Year	**Public**	**Government**	**Total**
1	$95,053,432	$7,046,950	$102,100,382
2	$584,394,262	$2,630,543	$587,024,805
3	$2,031,366,143	$4,941,427	$2,036,307,570
4	$4,106,424,873	$7,784,189	$4,114,209,062
5	$4,802,803,881	$8,900,527	$4,811,704,408
6	$5,917,019,480	$11,153,988	$5,928,173,468
7	$7,004,683,879	$13,603,261	$7,018,287,140
8	$4,229,652,383	$9,740,314	$4,239,392,697
9	$4,865,166,797	$11,556,342	$4,876,723,139
10	$5,582,583,879	$13,603,261	$5,596,187,140

Alternatives

[25] Base year (BY)

DoD considered and adopted several alternatives during the development of this rule that reduce the burden on defense contractors and still meet the objectives of the rule. These alternatives include: (1) maintaining status quo and leveraging only the current requirements implemented in DFARS provision 252.204-7019 and DFARS clause 252.204-7020 requiring DIB contractors and offerors to self-assess utilizing the DoD Assessment Methodology and entering a Basic Summary Score; (2) revising CMMC to reduce the burden for small businesses and contractors who do not process, store, or transmit critical CUI by eliminating the requirement to hire a C3PAO and instead allow self-assessment with affirmation to maintain compliance at CMMC Level 1, and allowing triennial self-assessment with an annual affirmation to maintain compliance for some CMMC Level 2 programs; (3) exempting contracts and orders exclusively for the acquisition of commercially available off-the-shelf items; and (4) implementing a phased implementation for CMMC.

In addition, the Department took into consideration the timing of the requirement to achieve a specified CMMC level: (1) at time of proposal or offer submission, (2) after contract award, (3) at the time of contract award, or (4) permitting government Program Managers to seek approval to waive inclusion of CMMC requirements in solicitations that involve disclosure or creation of FCI or CUI as part of the contract effort. Such waivers will be requested and approved by DoD in accordance with internal policies, procedures, and approval requirements. The Department ultimately adopted alternatives 3 and 4. The drawback of alternative 1 (at time of proposal or offer submission) is the increased risk for contractors since they may not have sufficient time to achieve the required CMMC level after the release of the solicitation. The drawback of alternative 2 (after contract award) is the increased risk to the Department with respect to the costs, program schedule, and uncertainty in the event the contractor is unable to achieve the required CMMC level in a reasonable amount of time given their current cybersecurity posture. This potential delay would apply to the entire supply chain and prevent the appropriate flow of CUI and FCI. The Department seeks public comment on the requirement to achieve a specified CMMC level by the time of contract award.

Benefits

The Department of Defense expects this proposed rule to protect DoD and industry from the loss of FCI and CUI, including intellectual property. The theft of intellectual property and sensitive unclassified information due to malicious cyber activity threatens U.S. economic security and national security. In 2010, the Commander of the U.S. Cyber Command and Director of the National Security Agency estimated the value of U.S. intellectual property to be $5 trillion and that $300 billion is stolen over networks annually[26]. The 2013 Intellectual Property Commission Report provided concurrence and noted that the ongoing theft represents "the greatest transfer of wealth in history." The report also highlighted the challenges of generating an exact figure because Government and private studies tend to understate the impacts due to inadequate data or scope, which is evidenced in subsequent analyses[27].

The responsibility of federal agencies to protect FCI or CUI does not change when such information is shared with DIB companies or organizations. A comparable level of protection is needed when FCI or CUI is processed, stored, or transmitted on contractor information

[26] https://www.govinfo.gov/content/pkg/CHRG-113hhrg86391/html/CHRG-113hhrg86391.htm
[27] https://www.nbr.org/program/commission-on-the-theft-of-intellectual-property/

systems.[28] The protection of FCI, CUI, and intellectual property on DIB company systems can directly impact the ability of the federal government to successfully conduct its essential missions and functions[29].

Malicious cyber actors have targeted and continue to target the DIB sector that consists of over 220,000 small-to-large sized entities that support the warfighter. In particular, actors ranging from cyber criminals to nation-states continue to attack companies and organizations that comprise the Department's multi-tier supply chain including smaller entities at the lower tiers. From at least January 2020, through February 2022, the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Cybersecurity and Infrastructure Security Agency (CISA) observed regular targeting of U.S. cleared defense contractors (CDCs) by Russian state-sponsored cyber actors. The actors have targeted sensitive, unclassified information, as well as proprietary and export-controlled technology. The acquired information provides significant insight into U.S. weapons platforms development and deployment timelines, vehicle specifications, and plans for communications infrastructure and IT. By acquiring proprietary internal documents and email communications, adversaries may be able to adjust their own military plans and priorities, hasten technological development efforts, inform foreign policymakers of U.S. intentions, and target potential sources for recruitment[30].

In addition to stealing intellectual property for military gains, Russia may conduct cyber-attacks against the U.S. for retaliatory purposes. On March 21, 2022, that the Biden-Harris Administration stated intelligence indicates that the Russian Government and Russian-aligned cybercrime groups have threatened to conduct cyber operations in retaliation for perceived cyber offensives against the Russian Government or the Russian people[31].

The aggregate loss of intellectual property and CUI from the DoD supply chain severely undercuts U.S. technical advantage, limits, and disrupts business opportunities associated with technological superiority, and ultimately threatens our national defenses and economy. By incorporating heightened cybersecurity standards into acquisition programs, the CMMC Program provides the Department assurance that contractors and subcontractors are meeting DoD's cybersecurity requirements and provides a key mechanism to adapt to an evolving threat landscape. This is critically important to the Department because the DIB is the target of increasingly frequent and complex cyberattacks by adversaries and non-state actors. Dynamically enhancing DIB cybersecurity to meet these evolving threats and safeguarding the information that supports and enables our warfighters is a top priority for the Department. The CMMC Program is a key component of the Department's DIB cybersecurity effort.

CMMC provides uniform and improved DoD cybersecurity requirements in three (3) levels, centered around the NIST cybersecurity guidelines. The Department is publishing with this rule supplemental guidance documents to assist the public and in particular, small businesses, with CMMC implementation, increasing the likelihood of successful implementation and strengthening cybersecurity across the DIB. CMMC decreases the burden and cost on companies

[28] https://www.cybernc.us/fci-cui/
[29] GAO Report to Congress, Defense Contractor Cybersecurity Stakeholder Communication and Performance Goals Could Improve Certification Framework, Dec 2021.
[30] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-047a
[31] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/

protecting FCI by allowing all companies at Level 1, and a subset of companies at Level 2, to demonstrate compliance through self-assessments. CMMC allows companies, under certain limited circumstances, to make a Plan of Action & Milestones (POA&M) to provide additional time to achieve final certification assessment. These key updates to CMMC benefit the DoD and our national interest by providing:

- improved safeguarding of competitive advantages through requirements flow-down to the DIB supply chain and protections for proprietary information and capabilities, and
- increased efficiency in the economy and private markets as a result of the streamlining of cybersecurity requirements, the resulting improvements in cybersecurity, and accountability across the supply chain.

In summary, the CMMC Program enforces and validates implementation of DoD's required cyber protection standards for companies in the DIB, preserving U.S. technical advantage. In addition, CMMC increases security for the most sensitive unclassified information by applying additional requirements. Implementation of CMMC will help protect DoD's sensitive unclassified information upon which DoD systems and critical infrastructure rely, making it vital to national security. CMMC is focused on securing the Department's supply chain, including the smallest, most vulnerable innovative companies. The security risks that result from the significant loss of FCI and CUI, including intellectual property and proprietary data, make implementation of the CMMC Program vital, practical, and in the public interest.