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

1. REASONS FOR THE ACTION 2
2. OBJECTIVES OF, AND LEGAL BASIS FOR, THE RULE 4
3. ANTICIPATED BENEFITS AND COSTS 6
   (a) Benefits 6
   (b) Costs 6
4. SMALL BUSINESS ENTITIES IMPACTED 8
   (a) Comparison to CMMC 1.0 Cost Analysis 8
   (b) Assumptions for CMMC 2.0 Cost Analysis 8
   Cost Analysis / Estimates by CMMC Level 11
5. RELEVANT FEDERAL RULES WHICH MAY DUPLICATE, OVERLAP, OR CONFLICT WITH THE RULE. 16
6. ALTERNATIVES 16
7. BENEFITS 17

INITIAL REGULATORY FLEXIBILITY ANALYSIS

Cybersecurity Maturity Model Certification (CMMC) Framework

32 CFR part 170; RIN 0790-AL49

This initial regulatory flexibility analysis has been prepared consistent with 5 U.S.C. 603.

1. Reasons for the Action

This proposed rule is necessary to create a secure and resilient supply chain, by addressing threats to the U.S. economy and national security from ongoing malicious cyber activities and preventing theft of hundreds of billions of dollars of U.S. intellectual property. The President's Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," emphasized that industrial security needs strengthening to ensure investments are not lost through intellectual property theft, among other supply chain risks.

Currently, the Federal Acquisition Regulation (FAR) and Defense FAR Supplement (DFARS) prescribe contract clauses intended to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within the Department of Defense (DoD) supply chain. 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. The FAR clause focuses on ensuring a basic level of cybersecurity hygiene and is reflective of actions that a prudent businessperson would employ.

In addition, DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires defense contractors and subcontractors to provide "adequate security" to process, store or transmit CUI on information systems or networks, and to report cyber incidents that affect these systems or networks. The clause states that to provide adequate security, the contractor shall implement, at a minimum, the security requirements in "National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Rev 2, Protecting CUI in Nonfederal Systems and Organizations." Contractors are also required to flow down DFARS clause 252.204-7012 to all subcontracts that involve CUI.

However, neither FAR 52.204-21 nor DFARS 252.204-7012, provide for DoD verification of a contractor's implementation of basic safeguarding requirements specified in FAR 52.204-21 nor the security requirements specified in DFARS 252.204-7012 which requires implementation of NIST SP 800-171 Rev 2 prior to contract award. Instead, DFARS clause 252.204-7012 requires prospective contractors or subcontractors to self-attest upon submission of their offer that they have implemented or will implement NIST SP 800-171 Rev 2 standards.

Findings from DoD Inspector General report (DODIG-2019-105 "Audit of Protection of DoD CUI 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. 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.

Due to these shortcomings and the associated risks to national security, the Department developed the Cybersecurity Maturity Model Certification (CMMC) Program to assess contractor and subcontractor implementation of DoD's required cybersecurity standards.

The Cybersecurity Maturity Model Certification (CMMC) Program verifies compliance with DoD cyber protection standards by defense contractors and subcontractors. It is designed to protect sensitive unclassified information that is shared by the Department with its contractors and subcontractors. The program incorporates a set of cybersecurity requirements into acquisition contracts and provides the Department increased assurance that contractors and subcontractors are meeting these requirements. The CMMC Program has three key features:

- **Tiered Model:** CMMC requires that companies implement cybersecurity standards at progressively advanced levels, depending on the type and sensitivity of the information. The program also sets forth the process for information flow down to subcontractors.

- **Assessment Requirement:** CMMC assessments allow the Department to verify the implementation of cybersecurity standards.

- **Implementation through Contracts:** Once CMMC is fully implemented, certain DoD contractors that handle sensitive unclassified DoD information will be required to achieve a particular CMMC level as a condition of contract award.

In September 2020, the DoD published an interim DFARS rule in the Federal Register (DFARS Case 2019-D041) that implemented the DoD's initial vision for the CMMC Program ("CMMC 1.0") and outlined the basic features of the program (tiered model, required assessments, and implementation through contracts). The interim rule became effective on November 30, 2020.

In March 2021, the Department initiated an internal review of CMMC's implementation, informed by more than 750 public comments in response to the interim DFARS rule. This comprehensive, programmatic assessment engaged cybersecurity and acquisition leaders within DoD to refine policy and program implementation.

In November 2021, the Department announced "CMMC 2.0," which is an updated program structure and revised requirements designed to achieve the primary goals of an internal DoD review of the CMMC Program. With the implementation of CMMC 2.0, the Department 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 at Level 1 and a subset of companies at Level 2 to demonstrate compliance through self-assessments.
- Increased oversight of professional and ethical standards of third-party assessors.

- Allowing companies, under limited circumstances, to make Plan of Action & Milestones (POA&M) to achieve certification.

In July 2022, the CMMC PMO met with the Office of Advocacy for the U.S. SBA to address the revisions planned in CMMC 2.0 that are responsive to prior SBA concerns. As a result of the alignment of CMMC 2.0 to NIST standards, 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.

2. Objectives of, and Legal Basis for, the Rule

The objective of this proposed rule (CMMC Program rule) is to provide the Department with increased assurance that a defense contractor can adequately protect sensitive unclassified information commensurate with the risk, accounting for information flow down to its subcontractors in a multi-tier supply chain. This rule meets the objective by providing a mechanism to assess contractor and subcontractor implementation of DoD's cyber security protection requirements for Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). Implementation of the CMMC Program is intended to address the following policy issues:

(a) Verification of a contractor's cybersecurity posture

Effective June 2016, FAR clause 52.204-7012 Basic Safeguarding of Contractor Information Systems, requires federal contractors and subcontractors to implement15 basic cyber hygiene requirements, as applicable, to protect contractor information systems that process, store, or transmit FCI.

December 31, 2017, was DoD's deadline for contractors to implement, as applicable, the cybersecurity protection requirements set forth in NIST SP 800-171 Rev 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, in accordance with DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. The current NIST 800-171A Assessment Guide states, "For the CUI security requirements in NIST Special Publication 800-171 Rev 2, nonfederal organizations describe in a system security plan, how the specified requirements are met or how organizations plan to meet the requirements [in a Plan of Action].[1]" NIST's process provides contractors with a tool to assess their security posture and decide if or when to mitigate the risks based upon the organizational risk tolerance. As such, a contractor is compliant with the NIST SP 800-171 Rev 2 standard if 10% of NIST SP 800-171 Rev 2 requirements are implemented and the other 90% are listed in a Plan of Action. As a result, at present, defense contractors and subcontractors can process, store, or transmit CUI without having implemented all security requirements set forth in the NIST SP 800-171 Rev 2 standard and without establishing concrete, prompt, and enforceable timelines for addressing shortfalls and gaps documented in the Plan of Action.

Findings from DoD Inspector General report (DODIG-2019-105 "Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems") indicated

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf

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 a third-party assessment requirement, as applicable, to verify defense contractors and subcontractors have implemented the required security requirements prior to award. CMMC also adds affirmation processes at every CMMC level requiring contractors and subcontractors to attest to compliance with CMMC's security requirements and then provide annual affirmations thereafter.

(b) Comprehensive implementation of cybersecurity requirements

Although the security requirements in NIST SP 800-171 Rev 2 address a range of threats, they do not sufficiently address Advanced Persistent Threats (APTs). An APT is an adversary that possesses sophisticated levels of expertise and significant resources, which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). To address APTs, NIST has published NIST SP 800-172, Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIS Special Publication 800-171 Rev 2. CMMC Level 3 provides for government assessment of a contractor's implementation of a defined subset of NIST SP 800-172 Enhanced Security Requirements with DoD predefined parameters and specifications.

(c) 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. Organizations Seeking Certification (OSCs) 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.

(d) Reduces Duplicate or Repetitive Assessments of our Industry Partners:

CMMC assessment results and contractor affirmations of compliance will be posted in the Supplier Performance Risk System (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 assessment requirements have been met for relevant contractor information system(s), avoids duplicative assessments, and eliminates the need for program level assessments, all of which decreases costs to both DoD and industry.

3. Anticipated Benefits and Costs

(a) Benefits

The CMMC Program validates implementation of DoD's required cyber protection standards for companies in the DIB. Furthermore, this rule benefits the efficient functioning of the economy and private markets for all sizes of companies, including the smallest, most vulnerable companies, by: (1) protecting DoD from the loss of FCI and CUI; (2) promoting improvements in cybersecurity and accountability across DoD supply chains; (3) promoting continued innovation by helping to prevent significant loss of revenue, benefits, and jobs to the companies involved in developing those innovations for DoD; (4) promoting U.S. technical advantage and superiority; and (5) improving the safeguarding of competitive advantages and protections for proprietary information and capabilities through requirements flow-down throughout the defense contractor supply chain.

(b) Costs

A Regulatory Impact Analysis (RIA) that includes a detailed discussion and explanation about the assumptions and methodology used to estimate the cost of this regulatory action is available at www.regulations.gov (search for "DoD-2021-OS-0063' click "Open Docket" and view "Supporting Documents"). The total estimated Public (large and small entities) and Government costs associated with this rule, calculated over a 20-year horizon in 2023 dollars at a 7 percent discount rate is provided as follows:

Total Estimated Cost of CMMC Requirements for the Public and the Government			
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

The following shows the estimated number of small entities[2] anticipated to pursue compliance or certification, at each CMMC level, over a phased implementation. These estimates were generated based upon prior year procurement data.

[2] Small entities are small business concerns.

Number of Small Entities Pursuing CMMC Over a Phased Implementation					
Year	**Level 1 Self-Assess**	**Level 2 Self-Assess**	**Level 2 Certification**	**Level 3 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
Total	**103,010**	**2,961**	**56,689**	**1,327**	**163,987**

The following is a summary of the estimated public costs of CMMC for small entities, per assessment of each contractor information system, at the required periodicity for each CMMC level.

Table 1 - Small Entities (per Assessment)				
Assessment Phase ($)	**Level 1 Self-Assessment**	**Level 2 Self-Assessment**	**Level 2 Certification**	**Level 3 Certification**
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 if allowed) will be documented in a Plan of Action and Milestones.

The following estimates are Small Entity Public and Government costs for CMMC requirements calculated over a 20-year horizon in 2023 dollars at a 7 percent discount rate.

Costs of CMMC Requirements for Small Businesses			
	Public	**Government**	**Total**
Annualized Costs	$2,616,493,297	$7,238,247	$2,623,731,544
Present Value Costs	$27,719,167,263	$76,682,096	$27,795,849,359

4. Small Business Entities Impacted

This rule will impact small businesses that do business with the Department of Defense as a prime or subcontractor, except for contracts or orders that are exclusively for COTS items, or valued at or below the micro-purchase threshold.

According to the Federal Procurement Data System (FPDS) there is an annual average of 30,145 unique small business contractors in DoD: FY 2019 (31,189), FY 2020 (29,166), FY 2021 (27,427) and FY 2022 (32,798).

Cost Assumptions and Analysis for CMMC 2.0

Complete details on CMMC requirements and associated costs, savings, and benefits of this rule are provided in the Regulatory Impact Analysis referenced in the Preamble. Key components of CMMC Program requirements are described in 32 CFR Subpart D.

(a) Comparison to CMMC 1.0 Cost Analysis

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 into 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.

(b) Assumptions for CMMC 2.0 Cost Analysis

In estimating the public cost for a small defense contractor to achieve CMMC compliance or certification at 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 companies and others 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 implementation (Non-recurring Engineering Costs (NRE)) or maintenance costs (Recurring Engineering (RE)[3]) for requirements prescribed in current regulations.

For CMMC Levels 1 and 2, cost estimates are based upon assessment, reporting, and affirmation activities which a contractor will take to validate conformance with existing cybersecurity requirements from the FAR clause 52.204-21, effective June 15, 2016, to protect FCI, and the 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 compliance with current 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. CMMC Level 3 security requirements are a selection of NIST SP 800-172 Enhanced Security Requirements as described in 32 CFR § 170.14(c)(4) and are not currently required through other regulations. DoD expects that CMMC Level 3 will 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 defined in FAR 52.204-21 and NIST SP 800-171 Rev 2 are assumed to have been 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 defined in FAR 52.204-21 and NIST SP 800-171 Rev 2 are assumed to have been 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 company 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

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

- Labor hour estimates for certified or authorized assessors to work with the small business to conduct the actual assessment

c) 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, where allowed, if applicable)
     - 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 a contractor or subcontractor to submit to SPRS an initial affirmation of compliance that the contractor information system is compliant with and will maintain compliance with the 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 comparable industry data and are defined in the table below.

Small Entities - Labor Rates Used for Estimate				
Code[4]	**Rate per Hour[5]**	**Description**	**Background / Years' Experience[6]**	**With Master's Degree[6]**
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[7]	$ 260.28	Cyber Subject Matter Expert	4 years	

[4] IT = Information Technology, MGMT = Management
[5] IT and MGMT rates represent an estimate for in-house labor and includes the labor rate plus fringe expenses
[6] 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.
[7] The ESP / C3PAO rate represents an estimate for outsourced labor and includes the labor rate, overhead expense, G&A expense, and profit

(c) Cost Analysis / Estimates by CMMC Level

CMMC Level 1 Self-Assessment and Affirmation Costs for Small Business 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 already implemented the basic safeguarding requirements set forth in FAR 52.204-21, which are the CMMC Level 1 security requirements.
- ***Self-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 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**: **$1,803**
    - 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[8] ($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] A person needs to enter the information into SPRS, which should only take five minutes.

8[9]		103,010	$615,679,258
9		103,010	$615,679,258
10		103,010	$615,679,258
Total	**103,010**		**$3,671,733,942**

CMMC Level 2 Self-Assessment and Affirmation Costs for Small Business Entities

The costs below account for a CMMC Level 2 Self-Assessment of the applicable contractor information system(s) with NIST SP 800-171 Rev 2 requirements based on assumptions defined above.

- ***Nonrecurring and recurring engineering costs****:* There are no nonrecurring or recurring engineering costs associated with a CMMC Level 2 Self-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 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 self-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**: **$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)
  - **Affirmation** – 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,

[9] 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.

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 and 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**

CMMC Level 2 Certification and Affirmation Costs for Small Business Entities

The costs below account for a CMMC Level 2 Certification assessment and affirmation costs of the applicable contractor information system(s) with NIST SP 800-171 Rev 2 requirements based on the assumptions defined above. CMMC Level 2 certification assessments require hiring a C3PAO to perform the assessment.

- ***Nonrecurring or recurring engineering costs****:* There are no nonrecurring or recurring engineering costs associated with CMMC Level 2 C3PAO Certification since it is assumed the contractor has implemented NIST SP 800-171 Rev 2 requirements.
- ***Assessment Costs and Initial Affirmation Costs****:* It is estimated that the cost to support a CMMC Level 2 C3PAO Certification and affirmation for a small entity is ***$101,752.** The three-year cost is $104,670 (as summarized in section 3(b) above, Table 1), 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 C3PAO Assessment Results**: **$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)
- **Affirmation** – initial affirmation post assessment: **$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 C3PAO 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 Affirmation 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**

CMMC Level 3 Certification and Affirmation Costs for Small Business Entities

A company pursuing a Level 3 Certification must have an active, final CMMC Level 2 Certification, and also must demonstrate compliance with CMMC Level 3, which includes implementation of a subset of security requirements from NIST SP 800-172 that have DoD predefined selections and parameters. CMMC Level 3 requires compliance with certain security requirements 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 subset of NIST SP 800-172 requirements. The cost estimates below account for time for a contractor or subcontractor to implement these security requirements and prepare for, support, and participate in a CMMC Level 3 assessment conducted by DoD. The company should keep in mind that the total cost of a Level 3 certification includes the cost of a Level 2 C3PAO assessment as well as the cost to implement and assess the requirements specific to Level 3. CMMC Level 3 is expected to affect a small subset of the DIB.

The estimated engineering costs per small entity associated with CMMC Level 3.

- ***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 C3PAO Certification 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 Level 3 assessment**: **$1,905**
    - A director (MGMT5) for 10 hours ($190.52/hr x 10hrs = $1,905)
  - **Phase 2: Conducting the Level 3 assessment**: **$1,524**
    - A director (MGMT5) for 8 hours ($190.52/hr x 8hrs = $1,524)
  - **Phase 3: Reporting of Level 3 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: Remediation (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)
  - **Affirmation** – initial affirmation post assessment: **$1,876**
- ***Reaffirmations:*** It is estimated that the costs to reaffirm a CMMC Level 3 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.

Yr	Entities Performing Triennial Certification including Initial Affirmation	Entities Re-affirmation Actions Only	Triennial Certification and Affirmation Total Cost	Non-recurring 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
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**

5. Relevant Federal rules which may duplicate, overlap, or conflict with the rule.

The rule does not duplicate, overlap, or conflict with any other Federal rules. Rather, this rule allows DoD to validate and verify that defense contractors and subcontractors have implemented existing cybersecurity requirements set forth in FAR clause 52.204-21 and in the NIST SP 800-171 Rev 2, which are intended to protect FCI and CUI during contract performance.

6. Alternatives

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 defense 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.

7. 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[10]. 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[11].

The responsibility of federal agencies to protect FCI or CUI does not change when such information is shared with defense companies or organizations. A comparable level of protection is needed when FCI or CUI is processed, stored, or transmitted on contractor information systems.[12] The protection of FCI, CUI, and intellectual property on defense company systems can directly impact the ability of the federal government to successfully conduct its essential missions and functions[13].

Malicious cyber actors have targeted and continue to target the DIB that consists of over 200,000 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

[10] https://www.govinfo.gov/content/pkg/CHRG-113hhrg86391/html/CHRG-113hhrg86391.htm
[11] https://www.nbr.org/program/commission-on-the-theft-of-intellectual-property/
[12] https://www.cybernc.us/fci-cui/
[13] GAO Report to Congress, Defense Contractor Cybersecurity Stakeholder Communication and Performance Goals Could Improve Certification Framework, Dec 2021.

military plans and priorities, hasten technological development efforts, inform foreign policymakers of U.S. intentions, and target potential sources for recruitment[14].

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[15].

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 defense contractors and subcontractors are the target of increasingly frequent and complex cyberattacks by adversaries and non-state actors. Dynamically enhancing defense contractors and subcontractors 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 standards. 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 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 defense contractor 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 defense contractors and subcontractors, 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,

[14] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-047a

[15] https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/

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.