PAPERWORK REDUCTION ACT REQUEST for 32 CFR

SUPPORTING STATEMENT - PART A

**Cybersecurity Maturity Model Certification (CMMC)**

**Enterprise Mission Assurance Support-Service (eMASS) Instantiation**

**Information Collection – 0704-XXXX**

1. Need for the Information Collection

 The CMMC Program provides for the assessment of contractor implementation of cybersecurity requirements to enhance confidence in contactor protection of unclassified information within the DoD supply chain. CMMC contractual requirements are implemented under a Title 48 acquisition rule, with associated rulemaking for the CMMC Program requirements (e.g., CMMC Scoring Methodology, certificate issuance, information accessibility) under a Title 32 program rule (32 CFR Part 170). The CMMC Title 32 program rule includes two separate information collection requests (ICR), one for the CMMC Program and this one for CMMC eMASS.

 The CMMC instantiation of eMASS is the electronic collection mechanism for collecting CMMC program data, which provides the Department of Defense (DoD) visibility of the CMMC Levels 2 and 3 certification assessment results.

 This information collection is necessary to support the implementation of the CMMC assessment process for CMMC Level 2 and Level 3 certification assessments, as defined in 32 CFR 170.17 and 170.18 respectively.

 The CMMC Level 2 certification assessment process is conducted by Certified Assessors, employed by CMMC Third-Party Assessment Organizations (C3PAOs). During the assessment process, Organizations Seeking Certification[[1]](#footnote-2) (OSCs) hire C3PAOs to conduct the third-party assessment required for certification. The CMMC Certified Assessors upload assessment data: pre-assessment and planning material (date and level of the assessment; C3PAO name and unique identifier; name and business contact information for each Assessor; all industry CAGE codes associated with the information systems addressed by the CMMC Assessment Scope; name, date, and version of the system security plan (SSP); the Title 32 program rule (32 CFR Part 170)), final assessment reports (assessment result for each requirement objective; POA&M usage and compliance, as applicable; and list of artifact names, the return values of the hashing algorithm, and the hashing algorithm used), and appropriate CMMC certificates of assessment (certification date, as applicable) into the CMMC instantiation of eMASS.

 The CMMC Level 3 certification assessment process is conducted by the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). DCMA DIBCAC assessors upload assessment data: pre-assessment and planning material (date and level of the assessment; name and business contact information for each Assessor; all industry CAGE codes associated with the information systems addressed by the CMMC Assessment Scope; name, date, and version of the system security plan (SSP); the Title 32 program rule (32 CFR Part 170)), final assessment reports (assessment result for each requirement objective; POA&M usage and compliance, as applicable; and list of artifact names, the return values of the hashing algorithm, and the hashing algorithm used), and appropriate CMMC certificates of assessment (certification date, as applicable) into the CMMC instantiation of eMASS.

2. Use of the Information

 **Accreditation Body (AB)**

 The Accreditation Body provides the CMMC Program Management Office (PMO) with current data on C3PAOs and Assessors, including authorization and accreditation records and status using the CMMC instantiation of eMASS.

 **CMMC Level 2 Certification Assessment**

1. The Level 2 Certification Assessment information collection reporting and recordkeeping requirements are addressed in a separate ICR for the CMMC Program. The requirement for the OSC to upload the affirmation in the Supplier Performance Risk System (SPRS) is addressed in the Title 48 acquisition rule and associated ICR.
2. Certified Assessors assigned by C3PAOs follow requirements and procedures as defined in 32 CFR 170.17 to conduct CMMC assessments on defense contractor information systems to determine conformance with the information safeguarding requirements associated with CMMC Level 2.
3. C3PAOs upload the data they collect into the CMMC instantiation of eMASS in a format compliant with the CMMC assessment data standard as set forth in eMASS\_CMMC\_Assessment\_Import\_Templates on the CMMC eMASS website: <https://cmmc.emass.apps.mil> and described in 32 CFR 170.9(b)(18). C3PAO assessment teams generate assessment data compliant with the CMMC assessment data standard, which comprises two JavaScript Object Notation (JSON) schemas: one for “pre-assessment” or planning data, and one for the assessment results. C3PAOs may develop or purchase any tool that is compliant with the data standard and DoD security requirements that generates pre-assessment data and assessment results in the required JSON file format. C3PAOs may also use spreadsheets that are compliant with the assessment data standard to submit the data. The generation and collection of the data that is submitted by the C3PAO is addressed in a separate ICR for the Title 32 CMMC Program rule. The C3PAO process to conduct a POA&M Close-out Assessment, where applicable, is the same as the initial assessment with the same information collection requirements.
4. The CMMC PMO will use the CMMC instantiation of eMASS for reporting and tracking metrics of the CMMC Program, including but not limited to, the number of OSCs, the number of certifications, the number of assessments conducted, and the number of POA&M successfully closed within the 180-day timeframe. The CMMC instantiation of eMASS will transfer assessment information to SPRS through an automated secure process, allowing DoD Contracting Officers to verify that offerors and contractors meet the required CMMC certification level at the time of contract award or option renewal.
5. The OSC is responsible for compiling relevant artifacts, this information collection is addressed in a separate ICR for the Title 32 CMMC Program rule. The C3PAO uploads the list of artifacts, hash of artifacts, and hashing algorithm used into the CMMC instantiation of eMASS. The OSC process to support a POA&M Close-out Assessment, where applicable, is the same as the initial assessment with the same information collection requirements.
6. If an OSC does not agree with the assessment results, it may formally dispute the assessment and initiate an Assessment Appeal process with the C3PAO who conducted the assessment. C3PAOs submit assessment appeals using eMASS. Appeals are tracked in the CMMC instantiation of eMASS and any resulting changes to the assessment results are uploaded into the CMMC instantiation of eMASS.

CMMC Level 3 Certification Assessment

1. The Level 3 Certification Assessment information collection reporting and recordkeeping requirements are addressed in a separate ICR for the Title 32 CMMC Program. The requirement for the OSC to upload the affirmation in SPRS is addressed in the Title 48 acquisition rule and associated ICR.
2. DCMA DIBCAC Assessors follow requirements and procedures as defined in 32 CFR 170.18 to conduct CMMC assessments on defense contractor information systems to determine conformance with the information safeguarding requirements associated with CMMC Level 3.
3. DCMA DIBCAC upload the data it collects into the CMMC instantiation of eMASS in a format compliant with the CMMC assessment data standard as set forth in eMASS\_CMMC\_Assessment\_Import\_Templates on the CMMC eMASS website: <https://cmmc.emass.apps.mil> and described in 32 CFR 170.9(b)(18). DCMA DIBCAC assessment teams generate assessment data compliant with the CMMC assessment data standard, which comprises two JavaScript Object Notation (JSON) schemas: one for “pre-assessment” or planning data, and one for the assessment results. The DCMA DIBCAC may develop or purchase any tool that is compliant with the data standard and DoD security requirements that generates pre-assessment data and assessment results in the required JSON file format. The DCMA DIBCAC may also use spreadsheets that are compliant with the assessment data standard to submit the data. The generation and collection of the data that is submitted by the DCMA DIBCAC is addressed in a separate ICR for the Title 32 CMMC Program rule. The DCMA DIBCAC process to conduct a POA&M Close-out Assessment, where applicable, is the same as the initial assessment with the same information collection requirements.
4. The CMMC PMO will use the CMMC instantiation of eMASS for reporting and tracking metrics of the CMMC Program, including but not limited to, the number of OSCs, the number of certifications, the number of assessments conducted, and the number of POA&M successfully closed within the 180-day timeframe. The CMMC instantiation of eMASS will transfer assessment information to SPRS through an automated secure process, allowing DoD Contracting Officers to verify that offerors and contractors meet the required CMMC certification level at the time of contract award or option renewal.
5. The OSC is responsible for compiling relevant artifacts, this information collection is addressed in a separate ICR for the Title 32 CMMC Program rule. The DCMA DIBCAC uploads the list of artifacts, hash of artifacts, and hashing algorithm used into the CMMC instantiation of eMASS. The OSC process to support a POA&M Close-out Assessment, where applicable, is the same as the initial assessment with the same information collection requirements.
6. If an OSC does not agree with the assessment results, it may formally dispute the assessment and initiate an Assessment Appeal process with the DCMA DIBCAC. DCMA DIBCAC submits assessment appeals using eMASS. Appeals are tracked in the CMMC instantiation of eMASS and any resulting changes to the assessment results are uploaded into the CMMC instantiation of eMASS.

3. Use of Information Technology

 CMMC assessment data and results are collected using information technology. C3PAOs and DCMA DIBCAC electronically upload assessment data and results into the CMMC instantiation of eMASS. The CMMC instantiation of eMASS electronically transfers certification results to SPRS. For Level 1 and 2 Self-Assessments, OSAs upload their assessment data directly into SPRS.

 Use of the CMMC instantiation of eMASS provides DoD visibility into the cybersecurity posture of the defense contractor supply chain and is the mechanism to generate reports on the health of the CMMC Ecosystem. SPRS is DoD's authoritative source for supplier and product performance information. Use of this electronic system to collect CMMC information eliminates the need for contractors to respond directly to multiple DoD requiring activities. SPRS serves as a single repository for Government access to CMMC assessment results. Modifications to information collections in SPRS will be addressed as part of the Title 48 acquisition rule and ICR.

4. Non-duplication

 The information obtained through this collection is unique and is not already available for use or adaptation from another cleared source.

5. Burden on Small Businesses

 A C3PAO may also be a small business. Efforts to minimize the burden on C3PAOs include the electronic collection of data using the CMMC instantiation of eMASS and providing Microsoft Excel spreadsheet templates.

6. Less Frequent Collection

 CMMC certifications last up to three years. The assessment frequency for each level was determined by the DoD based on the sensitivity of information processed, stored, or transmitted by the OSA at each level.

 DoD Program Managers use the CMMC information in SPRS to confirm the validity status of an OSA’s CMMC self-assessment or certification assessment prior to contract award. Rather than taking a contract-by-contract approach to securing Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), the OSA may obtain multiple contracts with a single CMMC self-assessment or certification assessment, thereby reducing the cost to both DoD and industry.

7. Paperwork Reduction Act Guidelines

 This collection of information does not require collection to be conducted in a manner inconsistent with the guidelines delineated in 5 CFR 1320.5(d)(2).

8. Consultation and Public Comments

 The Department consulted with members of the DIB Sector Coordinating Council (SCC), and government organizations including the DCMA DIBCAC and the Missile Defense Agency (MDA) in determining what data to collect in the CMMC instantiation of eMASS.

 The 60-Day Federal Register notice information is included in the preamble of the Title 32 CMMC Program proposed rule for public comment.

9. Gifts or Payment

 No payments or gifts are being offered to respondents as an incentive to participate in the collection.

10. Confidentiality

 The CMMC PMO coordinated with Defense Information Systems Agency (DISA) Privacy Office to validate compliance with all Privacy requirements, including the potential for there to be a Privacy Act Statement, System of Records Notice (SoRN), and/or Privacy Impact Assessment (PIA) associated with this collection. The PIA is available at <https://disa.mil/About/Legal-and-Regulatory/Privacy-Impact-Assessment>. The SoRN is available at https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-Component-Notices/DISA-Article-List.

 The CMMC PMO is also working with a Records Management point-of-contact to ensure records produced from this information collection are retained and disposed of according to a NARA approved Records Retention and Disposition Schedule. Records will be treated as permanent until the appropriate schedule is identified or approved.

11. Sensitive Questions

 No questions considered sensitive are being asked in this collection.

12. PART A & B: Respondent Burden and its Labor Costs

*Accreditation Body submission of C3PAO information in eMASS*. The Accreditation Body is one respondent, and it is estimated to make one response per day. This results in 240 annual responses (5 responses per week multiplied by 48 working weeks per year). It is estimated that the burden for the Accreditation Body to submit C3PAO information to the CMMC PMO in eMASS is approximately five minutes (0.08 hours) per response, or 19.2 hours annually (240 responses per year \* 0.08 hours per response). The hourly rate for this response is $84.91 per hour which is estimated based on the average of a GS-13 Step 1, Step 5, and Step 10, with a percentage added for fringe costs (employee benefits) and for minor overhead expenses (e.g., supervision and training). This results in a total estimated annual public cost of $1,630 = 240 annual responses \* 0.08 hour per response \* $84.91/hour.

|  |
| --- |
| **Estimation of Respondent Burden** |
| Number of respondents  | 1 |
| Responses per respondent  | 240 |
| Number of responses  | 240 |
| Hours per response  | .08 |
| Estimated hours | 19.2 |
| Cost per hour  | $84.91 |
| Annual public burden  | $1,630 |
| Cost per response | $7 |

*C3PAO submission of assessment data and results in eMASS*. The number of respondents is equal to the average number of entities expected to complete Level 2 Certification Assessments annually, or 10,942, with one response being provided per respondent. This results in 10,942 annual responses (10,942 respondents \* one response per respondent). It is estimated that the burden to submit assessment data and results in eMASS for Level 2 Certification Assessments is 15 minutes per response (0.25 hours), or 2,735.50 hours annually (10,942 annual responses \* 0.25 hours per response). The hourly rate for this response is $211.70 per hour which is a composite hourly rate derived from the detailed estimates in the CMMC cost estimate model. While the cost estimates in the model incorporates a variety of details (i.e., discrete numbers of entities by year and by type, detailed labor rates, fringe factors, and overhead factors), for purpose of this PRA estimate, one composite annual rate was derived from those details. This results in a total estimated annual public cost of $579,105 = 10,942 annual responses \* 0.25 hours/response \* $211.70/hour.

|  |
| --- |
| **Estimation of Respondent Burden** |
| Number of respondents  | 10,942 |
| Responses per respondent  | 1 |
| Number of responses  | 10,942 |
| Hours per response  | .25 |
| Estimated hours | 2,735.50 |
| Cost per hour  | $211.70  |
| Annual public burden  | $579,105  |
| Cost per response | $52.93 |

13. Respondent Costs Other Than Burden Hour Costs

Estimated government operational and maintenance costs for the annual support of the CMMC instantiation of eMASS. The estimated average annual amount is $2,731,861.

14. Cost to the Federal Government

*DCMA DIBCAC submission of assessment data and results in eMASS*. The number of respondents is equal to the average number of entities anticipated to complete Level 3 Certification Assessments annually, or 213, with one response being provided per respondent. This results in 213 annual responses (213 respondents \* one response per respondent). It is estimated that the burden to submit assessment data and results in eMASS for Level 3 Certification Assessments is 15 minutes per response (0.25 hours), or 53.25 hours annually (213 annual responses \* 0.25 hours per response).. The hourly rate for this response is $105.50 per hour which is a composite hourly rate derived from the detailed estimates in the CMMC cost estimate model. While the cost estimates in the model incorporates a variety of details (i.e., discrete numbers of entities by year and by type, detailed labor rates, fringe factors, and overhead factors), for purpose of this PRA estimate, one composite annual rate was derived from those details. This results in a total estimated annual public cost of $5,618 = 213 annual responses \* 0.25 hours/response \* $105.50/hour.

|  |
| --- |
| **Estimation of Government Burden** |
| Number of respondents  | 213 |
| Responses per respondent  | 1 |
| Number of responses  | 213 |
| Hours per response  | .25 |
| Estimated hours | 53.25 |
| Cost per hour  | $105.50 |
| Annual government burden  | $5,618 |
| Cost per response | $26.38 |

**ESTIMATION OF TOTAL PUBLIC AND GOVERNMENT BURDEN AND COST**

|  |
| --- |
| **Estimation of Total Public and Government Burden:** **Level 2 and Level 3 Certification Assessments[[2]](#footnote-3)** |
| Total Estimated Public Burden Hours (AB and C3PAO) | 2754.7 |
| Total Estimated Government Burden Hours | 53.25 |
| **Total Burden Hours** | 2807.95 |
| Total Annual Public Labor Cost (AB and C3PAO) (Average Over Phase-In Period) | $580,735 |
| Total Annual Government Labor Cost | $5,618 |
| Government Operational and Maintenance (Average Annual) | $2,731,861 |
| **Total Cost** | **$3,318,221** |

15. Reasons for Change in Burden

 This is a new collection with a new associated burden.

16. Publication of Results.

 The results of this information collection will not be published.

17. Non-Display of OMB Expiration Date

 DoD does not seek approval to omit the display of the expiration date for OMB approval of the information collection.

18. Exceptions to “Certification for Paperwork Reduction Submissions”

 DoD is not requesting any exceptions to the provisions stated in 5 CFR 1320.9.

1. An Organization Seeking Certification (OSC) is an entity seeking to contract, obtain, or maintain CMMC certification for a given information system at a particular CMMC Level. An OSC is also an OSA. [↑](#footnote-ref-2)
2. 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. [↑](#footnote-ref-3)