PAPERWORK REDUCTION ACT REQUEST for 32 CFR

SUPPORTING STATEMENT - PART A

**Cybersecurity Maturity Model Certification (CMMC) Program**

**Reporting and Recordkeeping Requirements**

**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), this one for the CMMC Program and one for CMMC eMASS.

 This information collection is necessary to support the implementation of the CMMC assessment process for Levels 2 and 3 certification assessment, 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 Level 3 certification assessment process is conducted by the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).

2. Use of the Information

**Level 1 and Level 2 CMMC Self-Assessments**

Organizations Seeking Assessment[[2]](#footnote-3) (OSAs) follow procedures as defined in 32 CFR

170.15(a)(1) and 170.16(a)(1) to conduct CMMC Level 1 and Level 2 Self-Assessments on their information systems to determine conformance with the information safeguarding requirements associated with a CMMC level.

The Level 1 and Level 2 Self-Assessment information collection reporting and

recordkeeping requirements will be included in a modification of an existing Defense Federal Acquisition Regulation Supplement (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 Title 48 acquisition rule.

**CMMC Level 2 Certification Assessment**

1. The Level 2 Certification Assessment information collection reporting and recordkeeping requirements are included in the Title 32 program rule with the exception of the requirement for the OSC to upload the affirmation in SPRS that is included in the Title 48 acquisition rule. Additionally, the information collection requirements for the CMMC instantiation of eMASS are addressed in a separate Title 32 program rule information collection request (ICR).
2. OSCs follow procedures as defined in 32 CFR 170.17 to prepare for CMMC Level 2 Certification Assessment.
3. 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. This is an assessment to validate implementation of the 110 security requirements from NIST SP 800-171 Rev 2.
4. Prospective C3PAOs must complete and submit the Standard Form (SF) 328 Certificate Pertaining to Foreign Interests (OMB control number 0704-0579) upon request from Defense Counterintelligence and Security Agency (DCSA).
5. C3PAOs must generate and collect pre-assessment and planning material (contact information for the OSC, information about the C3PAO and assessors conducting the assessment, the level of assessment planned, the CMMC Model and Assessment Guide versions, and assessment approach), artifact information (list of artifacts, hash of artifacts, and hashing algorithm used), final assessment reports, appropriate CMMC certificates of assessment, and assessment appeal information. C3PAOs submit the data they generate and collect into the CMMC instantiation of eMASS, the information collection required for this submission is addressed in a separate CMMC eMASS ICR for the Title 32 program rule.
6. OSCs may have a POA&M at CMMC Level 2 as addressed in 32 CFR 170.21. C3PAOs perform a POA&M closeout assessment. 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.
7. OSCs must retain artifacts used as evidence for the assessment for the duration of the validity period of the certificate of assessment, and at minimum, for six years from the date of certification assessment as addressed in 32 CFR 170.17(c)(4). The OSC is responsible for compiling relevant artifacts as evidence and having knowledgeable personnel available during the assessment. The organizational artifacts are proprietary to the OSC and will not be retained by the assessment team unless expressly permitted by the OSC. To preserve the integrity of the artifacts reviewed, the OSC creates a hash of assessment evidence (to include a list of the artifact names, the return values of the hashing algorithm, and the hashing algorithm used) and retains the artifact information for six years. The information obtained from the artifacts is an information collection and is provided to the C3PAO for uploading into the CMMC instantiation of eMASS (addressed in a separate CMMC eMASS ICR for the Title 32 program rule); the artifacts themselves are not an information collection. 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.
8. 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 (addressed in a separate CMMC eMASS ICR for the Title 32 program rule). 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.
9. C3PAOs maintain records for a period of six years of monitoring, education, training, technical knowledge, skills, experience, and authorization of each member of its personnel involved in inspection activities; contractual agreements with OSCs; any working papers generated from Level 2 Certification Assessments; and organizations for whom consulting services were provided as addressed in 32 CFR 170.9(b)(10).
10. The Accreditation Body provides the CMMC PMO with current data on C3PAOs, including authorization and accreditation records and status using the CMMC instantiation of eMASS (addressed in a separate CMMC eMASS ICR for the Title 32 program rule).
11. The Accreditation Body provides all plans related to potential sources of revenue, to include but not limited to: fees, licensing, processes, membership, and/or partnerships to the Government’s CMMC PMO as addressed in 32 CFR 170.8(b)(13).
12. CAICOs maintain records for a period of six years of all procedures, processes, and actions related to fulfillment of the requirements set forth in 32 CFR 170.10(b)(9).

CMMC Level 3 Certification Assessment

1. The Level 3 Certification Assessment information collection reporting and recordkeeping requirements are included in the Title 32 program rule with the exception of the requirement for the OSC to upload the affirmation in SPRS that is included in the Title 48 acquisition rule. Additionally, the information collection requirements for the CMMC instantiation of eMASS are addressed in a separate CMMC eMASS ICR for the Title 32 program rule.
2. OSCs follow procedures as defined in 32 CFR 170.18 to prepare for CMMC Level 3 Certification Assessment.
3. 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. This is an assessment to validation the implementation of the 24 selected security requirements from NIST SP 800-172. Because DCMA DIBCAC is a government entity, there are no public information collection requirements.
4. DCMA DIBCAC must generate and collect pre-assessment and planning material (contact information for the OSC, information about the assessors conducting the assessment, the level of assessment planned, the CMMC Model and Assessment Guide versions, and assessment approach), artifact information (list of artifacts, hash of artifacts, and hashing algorithm used), final assessment reports, appropriate CMMC certificates of assessment, and assessment appeal information. DCMA DIBCAC submits the data it generates and collects into the CMMC instantiation of eMASS (addressed in a separate CMMC eMASS ICR for the Title 32 program rule).
5. OSCs may have a POA&M at CMMC Level 3 as addressed in 32 CFR 170.21.
DCMA DIBCAC performs a POA&M closeout assessment. 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.
6. OSCs must retain artifacts used as evidence for the assessment for the duration of the validity period of the certificate of assessment, and at minimum, for six years from the date of certification assessment as addressed in 32 CFR 170.18(c)(4). The OSC is responsible for compiling relevant artifacts as evidence and having knowledgeable personnel available during the assessment. Assessors will not permanently retain assessment artifacts. To preserve the integrity of the artifacts reviewed during the assessment, the OSC creates a hash of assessment evidence (to include a list of the artifact names, the return values of the hashing algorithm, and the hashing algorithm used) and retains the artifact information for six years. The information obtained from the artifacts is an information collection and DCMA DIBCAC uploads the information into the CMMC instantiation of eMASS (addressed in a separate CMMC eMASS ICR for the Title 32 program rule); the artifacts themselves are not an information collection. 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.
7. If an OSC does not agree with the assessment results, it may formally dispute the assessment and initiate an Assessment Appeal process with DCMA DIBCAC. DCMA DIBCAC submits assessment appeals using eMASS (addressed in a separate CMMC eMASS ICR for the Title 32 program rule). Appeals are tracked in the CMMC instantiation of eMASS and any resulting changes to the assessment results are uploaded into CMMC eMASS.
8. DCMA DIBCAC maintains records for a period of six years of monitoring, education, training, technical knowledge, skills, experience, and authorization of each member of its personnel involved in inspection activities and working papers generated from Level 3 Certification Assessments.

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 (addressed in a separate CMMC eMASS ICR for the Title 32 program rule). 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 in 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

 For Level 1 and 2 Self-Assessments, OSAs must report annually and triennially, respectively. Level 2 and Level 3 certification assessments must be conducted every three years by a C3PAO or DCMA DIBCAC, respectively. At all levels, an annual affirmation is required. In all cases, the burden applied to small business is the minimum consistent with applicable laws, Executive orders, regulations, and prudent business practices.

 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 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 Program Management Office (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 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

 The Level 1 and Level 2 Self-Assessment information collection reporting and recordkeeping requirements for the CMMC Program 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 Title 48 acquisition rule.

The public burden costs associated with Level 2 and Level 3 Certification Assessment information collection reporting and recordkeeping requirements for the CMMC Program are addressed here, with the exception of the eMASS reporting requirements which will be addressed as part of a separate CMMC eMASS ICR for the Title 32 program rule. Respondent burden and cost for these information collection reporting and recordkeeping requirements are as follows:

|  |  |  |
| --- | --- | --- |
|  |  | **LEVEL 2 AND LEVEL 3 CERTIFICATION ASSESSMENT PUBLIC RESPONDENT BURDEN AND LABOR COSTS** |
| **Collection Instrument and Rule Citation** | **Entity Type** | **Number of Responses[[3]](#footnote-4)**  | **Hours per Response[[4]](#footnote-5)** | **Burden Hours** | **Hourly Rate[[5]](#footnote-6)** | **Burden Per Response** | **Total Burden** |
| Level 2 | OSC (& hired C3PAO[[6]](#footnote-7)) - Small | 8,098 | 417.83 |  3,383,587.34  | $239.89  | $100,233  | $811,688,767  |
| Certification Assessment§170.17 (a) | OSC (& hired C3PAO7) - Other Than Small | 2,844 | 833.83 |  2,371,412.52  | $131.44  | $109,599  | $311,698,462  |
| Level 3 | OSC - Small | 190 | 42.08 |  7,995.20  | $170.48  | $ 7,174  | $1,363,022  |
| Certification Assessment§170.18 (a) | OSC - Other Than Small | 23 | 384.08 |  8,833.84  | $ 94.53  | $36,307  | $ 835,063  |

13. Respondent Costs Other Than Burden Hour Costs

 Non-Recurring and Recurring Engineering estimated costs are included for Level 3 Certification Assessments. Non-Recurring Engineering reflects a one-time cost consisting of hardware, software, and the associated labor to implement the same. Recurring Engineering reflects annually recurring fees and associated labor for technology refresh. The estimated amounts below are average annual amounts for all entities as indicated.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | **RESPONDENT COSTS OTHER THAN BURDEN** |
| RuleCitation | Collection Requirement | Entity Type | Non-Recurring Cost | Recurring Cost | Total Costs |
| §170.18 (a) | Level 3 | OSC - Small |  $ 513,000,000  |  $ 93,100,000  |  $ 606,100,000  |
|  | Certification | OSC - Other Than Small |  $ 485,300,000  |  $ 94,760,000  |  $ 580,060,000  |
|  |  | **TOTAL** |  |  |  **$ 1,186,160,000**  |

Travel costs for C3PAO assessors may represent an additional cost for respondents.

14. Cost to the Federal Government

 The government burden costs associated with Level 3 Certification Assessment information collection reporting and recordkeeping requirements for the CMMC Program are addressed here, with the exception of the eMASS reporting requirements which will be addressed as part of a separate CMMC eMASS ICR for the Title 32 program rule. Respondent burden and cost for these information collection reporting and recordkeeping requirements are as follows:

|  |  |  |
| --- | --- | --- |
|  |  | **LEVEL 3 CERTIFICATION ASSESSMENT GOVERNMENT RESPONDENT BURDEN AND LABOR COSTS** |
| **Collection Instrument and Rule Citation** | **Entity Type** | **Number of Responses[[7]](#footnote-8)**  | **Hours per Response[[8]](#footnote-9)** | **Burden Hours** | **Hourly Rate[[9]](#footnote-10)** | **Burden Per Response** | **Total Burden** |
| Level 3 | OSC (& DCMA DIBCAC[[10]](#footnote-11)) - Small | 190 | 117.75 |  22,372.50  | $108.47  | $ 12,772  | $2,426,745  |
| Certification Assessment§170.18 (a) | OSC (& DCMA DIBCAC12) - Other Than Small | 23 | 435.75 |  10,022.25  | $ 81.01  | $35,300  | $ 811,902  |

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

|  |
| --- |
| **Estimation of Total Public and Government Burden:** **CMMC Level 2 and Level 3 Certification Assessments[[11]](#footnote-12)** |
| Total Estimated Public Burden Hours | 5,771,828.9 |
| Total Estimated Government Burden Hours | 32,394.75 |
| **Total Burden Hours** | **5,804,223.65** |
| Total Annual Public Labor Cost (Average Over Phase-In Period) | **$1,125,585,313** |
| Total Annual Government Labor Cost | $3,238,648 |
| Respondent Non-Recurring and Recurring (Average Annual) | $1,186,160,000 |
| **Total Cost** | **$2,314,983,961** |

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. An Organization Seeking Assessment (OSA) is an entity seeking to conduct, obtain, or maintain a CMMC assessment for a given information system at a particular CMMC Level. The term OSA includes all OSCs. [↑](#footnote-ref-3)
3. Respondent is equivalent to an entity; an entity provides one response annually. [↑](#footnote-ref-4)
4. Hours per Response represents the estimated burden hours to complete the indicated assessment. [↑](#footnote-ref-5)
5. Hourly Rate represents a composite hourly rate derived from the detailed type of labor and associated rates estimated in the CMMC cost estimate model. [↑](#footnote-ref-6)
6. The entity type refers to the size of the OSC as either Small or Other Than Small; the entity type does not refer to the size of the C3PAO. [↑](#footnote-ref-7)
7. Respondent is equivalent to an entity; an entity provides one response annually. [↑](#footnote-ref-8)
8. Hours per Response represents the estimated Government burden hours to complete the indicated assessment. [↑](#footnote-ref-9)
9. The Hourly Rate represents a composite hourly rate derived from the detailed type of Government labor and associated rates estimated in the CMMC cost estimate model. [↑](#footnote-ref-10)
10. The entity type refers to the size of the OSC as either Small or Other Than Small; the entity type does not refer to the size of DCMA DIBCAC. [↑](#footnote-ref-11)
11. 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 Title 48 acquisition rule. [↑](#footnote-ref-12)