SUPPORTING STATEMENT - PART A

Cybersecurity Maturity Model Certification (CMMC) Program

Reporting and Recordkeeping Requirements

Information Collection – 0704-0677

1. Need for the Information Collection

This information collection request describes the documentation requirements discussed in the final Cybersecurity Maturity Model Certification (CMMC) program rule published at 89 FR 83092, specifically 32 CFR 170.17 and 170.18. These requirements are needed to support the implementation of the CMMC assessment process for Levels 2 and 3 certification assessments. As discussed in the rule, a Level 2 certification assessment process is conducted by CMMC Certified Assessors (CCAs), employed by CMMC Third-Party Assessment Organizations (C3PAOs). During the assessment process, Organizations Seeking Certification[1] (OSCs) hire C3PAOs to conduct the third-party assessment required for certification.

The Level 3 certification assessment process is conducted on OSCs by the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).

The CMMC rule places recordkeeping requirements on several entities involved in the assessment process. These include the maintenance of assessment related records, records developed in the process of accrediting C3PAOs, and CMMC Accreditation Body plans related to potential sources of revenue.

[1] An Organization Seeking Certification (OSC) means the entity seeking to undergo certification assessment for a given information system for the purposes of achieving and maintaining the CMMC Status of Level 2 (C3PAO) or Level 3 (DIBCAC). An OSC is also an OSA.

2. Use of the Information

OSC and C3PAO Requirements for CMMC Level 2 Certification Assessment

To comply with CMMC Level 2 certification assessment requirements, OSCs undergo a Level 2 certification assessment performed by an accredited C3PAO. To achieve a CMMC status of either Conditional or Final Level 2, the OSC must complete the assessment and achieve a MET result for all security requirements specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Rev 2. To maintain compliance with the requirements for a CMMC status of Level 2, the Level 2 certification assessment must be performed every three years.

As discussed in the rule, CCAs assigned by C3PAOs follow the requirements and procedures 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 Level 2 certification assessment and validate implementation of the 110 security requirements from NIST SP 800-171 Rev 2. The Level 2 certification assessment must be scored in accordance with the CMMC Scoring Methodology described in 32 CFR 170.24.

OSCs must provide C3PAOs with the information necessary to perform the assessment, including that which is necessary to generate pre-assessment and planning materials and prepare final assessment reports. OSCs must also retain all 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 hash file name and resulting hash string obtained from the artifacts is an information collection and is provided to the C3PAO.

OSCs may have a Plan of Action and Milestones (POA&M) at Level 2 certification assessment as addressed in 32 CFR 170.21. C3PAOs perform a POA&M closeout assessment. The C3PAO process to conduct a POA&M closeout assessment, when applicable, is the same as the initial assessment with the same information collection requirements from the OSCs.

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 that conducted the assessment.

OSC Requirements for CMMC Level 3 Certification Assessment

To comply with CMMC Level 3 certification assessment requirements, OSCs undergo a Level 3 certification assessment performed by DCMA DIBCAC. The OSC must achieve a CMMC Status of Final Level 2 on the Level 3 CMMC Assessment Scope prior to initiating a Level 3 certification assessment. To achieve a CMMC status of Level 3, the OSC must complete the assessment, achieving a "MET" result for all security requirements specified in Table 1 of 170.14(c)(4). To maintain compliance with the requirements for a CMMC status of Level 3, the assessment must be performed every three years for all information systems within the Level 3 CMMC Assessment Scope.

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 validate the implementation of the 24 selected security requirements from NIST SP 800-172.

The OSC initiates a Level 3 certification assessment by emailing a request to DCMA DIBCAC at: dcma_dibcac_cmmc@mail.mil. The request must include the Level 2 certification assessment unique identifier. DCMA DIBCAC will validate the OSC has achieved a CMMC Status of Level 2 and will contact the OSC to schedule their Level 3 certification assessment. OSCs must provide DCMA DIBCAC with the information necessary to perform the assessment, including that which is necessary to generate pre-assessment and planning materials and prepare final assessment reports. As part of the certification process, 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. Final assessment results are communicated to the OSC through a CMMC Assessment Findings Report.

OSCs may have a POA&M at CMMC Level 3. DCMA DIBCAC performs the POA&M closeout assessment. The OSC process to support a POA&M closeout assessment, when

applicable, is the same as the initial assessment with the same information collection requirements.

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.

Associated Recordkeeping Requirements

Per 32 CFR 170.9(b)(9), C3PAOs must maintain all assessment related records for a period of six years. Such records include any materials generated by the C3PAO in the course of an assessment, any working papers generated from Level 2 certification assessments; and materials relating to monitoring, education, training, technical knowledge, skills, experience, and authorization of all personnel involved in assessment activities; contractual agreements with OSCs; and organizations for whom consulting services were provided.

Per 32 CFR 170.8(b)(13), the Accreditation Body must provide all plans related to potential sources of revenue, to include but not limited to: fees, licensing, processes, membership, and/or partnerships to the Government CMMC Program Management Office (PMO).

The CMMC Assessor and Instructor Certification Organization (CAICO) must 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.

3. Use of Information Technology

C3PAOs and DCMA DIBCAC electronically upload assessment data and results into the CMMC instantiation of eMASS which is covered under OMB control number 0704-0676. Information on the eMASS collection, including all supporting documentation, can be accessed

at https://www.reginfo.gov/public/do/PRAMain by typing in either the OMB control number or the name of the collection. eMASS electronically transfers certification results to the Supplier Performance Risk System (SPRS), which is covered under OMB control number 0750-0004. For Level 1 and 2 self-assessments, Organizations Seeking Assessment[2] (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

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

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 by the OSC is required. In all cases, the burden applied to small businesses 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 and providing Microsoft Excel spreadsheet templates.

[2] An Organization Seeking Assessment (OSA) means the entity seeking to undergo a self-assessment or certification assessment for a given information system for the purposes of achieving and maintaining any CMMC Status. The term OSA includes all OSCs.

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.

The 60-Day Federal Register Notice (FRN) was published as part of the proposed rule, which published on Tuesday, December 26, 2023. The proposed rule citation is 88 FR 89058. Comments pertaining to the cost and burden of the collection were discussed as part of the final rule for the CMMC program.

The 30-Day FRN was published on Friday, June 21, 2024. The FRN citation is 89 FR 52034. One public comment was received, and the Department's response is provided as a supplementary document in the information collection request package.

9. Gifts or Payment

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

10. Confidentiality

A Privacy Act Statement and a Privacy Impact Assessment is not required for this collection because we are not requesting individuals to furnish personal information.

A System of Record Notice (SORN) is not required for this collection because records are not retrievable by PII.

The OSD Records Manager signed a Memorandum for the Record, dated 9 Oct 2024 and included in this information collection request, that includes the Records Disposition Schedule for SPRS addressed by the National Archives and Records Administration (NARA), General Records Schedule 3.2, Information Systems Security Records, Item 010, Systems and Data Security Records. Records produced from this information collection will be retained and disposed of according to this NARA approved Records Retention and Disposition Schedule. This disposition will be included in the next update of OSD Records Disposition Schedules and posted to https://www.esd.whs.mil/RIM/.

11. Sensitive Questions

No questions considered sensitive are being asked in this collection.

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

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. 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]**	**Hours per Response[4]**	**Burden Hours**	**Hourly Rate[5]**	**Burden Per Response**	**Total Burden**
Level 2 certification assessment §170.17 (a)	OSC (& hired C3PAO[6]) - Small	8,098	417.83	3,383,587.34	$239.89	$100,233	$811,688,767
	OSC (& hired C3PAO[6]) - Other Than Small	2,844	833.83	2,371,412.52	$131.44	$109,599	$311,698,462
Level 3 certification assessment §170.18 (a)	OSC - Small	190	42.08	7,995.20	$170.48	$ 7,174	$ 1,363,022
	OSC - Other Than Small	23	384.08	8,833.84	$ 94.53	$36,307	$ 835,063
TOTAL		**11,155**		**5,771,828.90**			**$1,125,585,314**

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

[3] Respondent is equivalent to an entity; an entity provides one response annually.
[4] Hours per Response represents the estimated burden hours to complete the indicated assessment.
[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.
[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.

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		
Rule Citation	Collection Requirement	Entity Type	Non-Recurring Cost	Recurring Cost	Total Costs
§170.18 (a)	Level 3 Certification	OSC - Small	$ 513,000,000	$ 93,100,000	$ 606,100,000
		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. 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	**Entity Type**	**Number of Responses[7]**	**Hours per Response[8]**	**Burden Hours**	**Hourly Rate[9]**	**Burden Per**	**Total Burden**

[7] Respondent is equivalent to an entity; an entity provides one response annually.
[8] Hours per Response represents the estimated Government burden hours to complete the indicated assessment.
[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.

and Rule Citation						Response	
Level 3 certification assessment §170.18 (a)	OSC (& DCMA DIBCAC[10]) - Small	190	117.75	22,372.5	$108.47	$12,772	$2,426,745
	OSC (& DCMA DIBCAC[10]) - Other Than Small	23	435.75	10,022.25	$ 81.01	$35,300	$ 811,902
TOTAL		**213**		**32,394.75**			**$3,238,647**

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. Aggregate information such as the total number of completed assessments submitted to DoD may be provided in Congressional justification materials or to the Office of Management and Budget (OMB).

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.

[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.