OMB Control Number 0704-0677 – Cybersecurity Maturity Model Certification (CMMC) Program Reporting and Recordkeeping Requirements Information Collection

DoD Responses to public comments received on the 30-Day Federal Register Notice (Docket ID DOD-2023-OS-0063)

1. **Comment**: **The "Comment" button is not active on the website.** After following the directions, the web entry does not have a "Comment" button. The entries before and after do. I have already submitted a question to the listed POC on this.

   Response: **Reject. See reasoning.**
   Reasoning: The comment button is active and functioning (8 July).

2. **Comment**: **Level 1 Self-Assessments are not addressed.** Level 1 also contains an information collection requirement from the USG, that says, "At Level 1, CMMC adds a requirement for contractors and applicable subcontractors to verify through self-assessment that all applicable security requirements outlined in FAR clause 52.204-21 have been implemented. This self-assessment must be performed annually and the results must be entered electronically in the Supplier Performance Risk System (SPRS)" *32CFR170 CMMC 2.0 Overview of Proposed Rule 1.b.* The Level 1 collection requirement should also be addressed.
   - The DoD estimated in 32CFR170 and the table included below that 139,201 respondents would be required and that submission would be annual.
   - The DoD did not explicitly estimate the hours required however they did estimate the cost required as $5,977. Given an *average* of the labor rates contained in table 10 of $130.47 per hour, we conclude that this is 45.811 hours of effort per respondent and that this in turn results in an additional 6,376,937 Annual Burden Hours.

   Response: **Reject. See reasoning.**
   Reasoning: CMMC Level 1 is not included in the Title 32 CFR PRA Information Collection Requirement (ICR), as it is addressed in another ICR under the

companion Title 48 CFR acquisition rule, Assessing Contractor Implementation of Cybersecurity Requirements, as addressed in this ICR in Footnote 11 (p. 14). The commenter referenced Table 10 (in the preamble) to compute his estimate. Table 10 is an example listing of labor rates for Other than Small Entities for a CMMC assessment, the average of which does not apply for CMMC Level 1 or this ICR. The paragraphs following Tables 10 and 11 (p. 295, preamble) correctly address the CMMC Level 1 Self-Assessment costs. No edit is needed to the PRA ICR for CMMC Level 1 Self-Assessment.

3. **Comment**: **Level 2 Self-Assessments are not addressed.** Level 2 self-assessments are separate from certification assessments and fall on a different set of estimated companies as outlined in 32CFR170. These also constitute an information collection activity. Self-assessments should be carried out in the same manner as certification assessments just conducted solely by the OSC so we would expect that the
    - The DoD estimated in 32CFR 170 and the table included below that 4,000 respondents would be required and that submission would be triennially.
    - The DoD did not explicitly estimate the hours required however they did estimate the cost required as $48,827 per respondent. Given an *average* of the labor rates contained in Table 10 of $130.47 per hour, we conclude that this is hours of effort per respondent and that this in turn results in 374.239 hours per respondent and adds an additional 1,496,956 Annual Burden Hours.

Response: **Reject. See reasoning.**

Reasoning: Same rationale as provided for Comment #2. CMMC Level 2 Self-Assessment is not included in the Title 32 CFR PRA Information Collection Requirement (ICR), as it is addressed in another ICR under the companion Title 48 CFR acquisition rule, Assessing Contractor Implementation of Cybersecurity Requirements, as referenced in ICR Footnote 11 (p. 14). The commenter references cost estimates from the Regulatory Impact Analysis (RIA), which are not the same as the PRA ICR estimates. The ICR includes annual computed estimates for the

information collections, while the RIA addresses cumulative averages over the stated seven-year period. As referenced by the commenter, Table 10 is an example listing of labor rates for Other than Small Entities for a CMMC assessment, the average of which does not apply for CMMC Level 2 Self-Assessments or this ICR. The paragraphs following Tables 10 and 11 (p. 299 in preamble) correctly address the CMMC Level 2 Self-Assessment costs. No edit is needed to the PRA ICR for CMMC Level 2 Self-Assessment.

4. **Comment**: **Level 2 Certification Assessments.** From the ICR it states:
    - "Number of Respondents: 10,942.
    - Responses per Respondent: 1.
    - Annual Responses: 10,942.
    - Average Burden per Response: 525.955 hours.
    - Annual Burden Hours: 5,754,999.61."

    The number of respondents does not match the DoD's estimated number of respondents as outlined in 32CR170 proposed rule. Under the "Impact and Cost Analysis of CMMC 2.0" in the 32CFR170 proposed rule, it presents the following Table 3:

Table 3 - Estimated Number of Entities by Type and Level

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

This indicates that the number of DoD estimated Level 2 certifications is 76,598. Elsewhere in the proposed regulation we see that these certifications are valid for three years and therefore the annual respondents required should be 25,533 instead

of the 10,942 listed here. The annual burden of hours should be adjusted accordingly to 13,429,209 hours.

Using our methodology for estimating the DoD input for Average Burden per Response, and applying that to the Level 2 Certification assessments, we see that in Table 7 of 32CFR170 they estimated the Level 2 certification cost as $117,768. Applying the $130.47 average rate we arrive at 902.644 burden hours. Given that these numbers include both OSC preparation activities, which will likely be extensive, and the C3PAO activities to actually conduct the assessment, we would submit that neither calculation overestimates the actual work that will be required in preparing for and conducting assessments. We acknowledge that work preparing for assessments and implementing security controls (not covered) would be difficult to sort in any meaningful way when looking at activities conducted by OSCs.

Bottom line. The number of respondents does not match DoD estimates in 32CFR170 proposed rule. The Average Burden per Response hour is subject to broad interpretation, however, if there is an error, they are on the low side as submitted in the ICR.

Response: **Reject. See reasoning.**

Reasoning: The CMMC Level 2 Certification Assessment total of 76,598 shown in Table 3 in the preamble (p. 287) is a cumulative approximated number across seven years, not three years, as suggested by the commenter (76,598 divided by 7 = 10,942). The number of respondents does match the DoD's estimated number of respondents and is correct. The estimates in the PRA ICR are *annual* estimates for the total number of respondents. (See Footnote #58: Respondent is equivalent to an entity; an entity provides one response annually.) No edit is needed to the PRA ICR for CMMC Level 2 Certification Assessments.

5. **Comment**: **Level 3 Certification Assessments.** From the ICR it states:
    - Number of Respondents: 213

- Responses per Respondent: 1
- Annual Responses:213
- Average Burden per Response: 79.01 hours
- Annual Burden Hours: 16,829.13

Again, the number of respondents does not match the DoD's estimated number of respondents as outlined in 32CR170 proposed rule. Per Table 3 of 32CFR170, we can see that the DoD estimates that 1487 companies will require Level 3 certification every 3 years, or 496 annually. Sticking with the DoD's estimate of Average Burden hours per response we calculate 39,162.622 as the additional burden hours.

In this case, we submit that the DoD however has underestimated the hours required for preparation and evidence collection for the Level 3 certification. Although this certification contains fewer controls, these controls are more challenging by design. We submit that these requirements amount to a quarter-year effort additionally and specific to level three at a minimum. 504 Average Burden Hours per Response.

Response: **Reject. See reasoning.**

Reasoning: Same rationale as response above. The CMMC Level 3 Certification Assessment total of 1,487 shown in Table 3 is a cumulative approximated number across the stated seven-year period, not three years, as suggested by the commenter: 1,487 divided by 7 is approximately 213 per year. The number of respondents is correct and matches DoD's estimated number of respondents. No edits are needed in the PRA ICR for CMMC Level 3.

6. **Comment**: **Typo.** The ICR States, "DCMA DIBCAC submits the data it generates and collects into the CMMC instantiation of." Truncating the sentence.
   Coordinator Recommended Change: The likely conclusion of this sentence is "eMASS."

<u>Response</u>: **Accept.**