CMMC Accreditation Body RFI Questions and Draft Responses

Question 1: Is this a new requirement or contract renewal?

- Answer: This is not a contract renewal and the government anticipates that no contract will result from this RFI. The purpose of the RFI is to obtain information.

Question 2: If renewal, what is current contract number?

- Answer: Please refer to the answer associated with Question 1.

Question 3: When does the Government anticipate the RFP release?

- Answer: Please refer to the answer associated with Question 1.

Question 4: Will the RFP solicitation number be changed?

- Answer: Please refer to the answer associated with Question 1.

Question 5: When does the Government anticipate the award - FY19?

- Answer: Please refer to the answer associated with Question 1.

Question 6: Do you know what the process is to become a certified 3rd party to perform CMMC accreditations?

- Answer: That process has yet to be determined. It is anticipated that this process will be determined by the CMMC Accreditation Body.

Question 7: The RFI states that "*The working estimate for the number of organizations requiring CMMC certifications is 300,000*". To support this large number of organizations requiring CMMC certifications, how many Third Party Assessment Organizations (C3PAOs) are estimated to be accredited by the CMMC Accreditation Body?

- Answer: There is no estimate at this time. The number of C3PAOs will depend upon the size and capacity of these organizations, and it is anticipated that it will ramp up over time.

Question 8: Once a C3PAO is accredited/certified at a specified level by the CMMC Accreditation Body, what is the re-assessment cycle (Continuous Monitoring) to keep the C3PAO at that CMMC at a specified level? This will help better understand the scope, size and workload of the CMMC Accreditation Body activities for re-assessments.

- Answer: The CMMC Accreditation Body will establish the requirements for C3PAO recertification.

Question 9: The RFI states that "*Each assessment will be conducted by a credentialed independent assessor working for an accredited C3PAO under the oversight of the CMMC Accreditation Body*". Is the intent of the Govt. to have the Accreditation Body accredit individuals as independent CMMC Assessors regardless of their employment status with an accredited C3PAO or not?
Once an individual is accredited as an independent assessor (by the CMMC Accreditation Body), will the individual be capable of conducting assessments for a different C3PAO if the employment situation changes?
Please clarify.

- Answer: The CMMC Accreditation Body will establish requirements for individual assessors who are either employed by a certified C3PAO or work independently.

Question 10: The RFI states that "*The working estimate for the number of organizations requiring CMMC certifications is 300,000*". In the future, if organizations/companies (not within the 300,000 estimate) who need to achieve CMMC certification (due to non-DoD agency requirements or other private sector compliance needs), will the CMMC Accreditation Body be the only organization responsible for managing, operating and sustaining the CMMC program for such companies?

- Answer: See response to Question 13. The initial focus of CMMC is for the DIB sector that supports the DoD.

Question 11: Do you have an estimate of the number of companies that you expect will seek accreditation in 2020, the first year of CMMC implementation?

- Answer: Not at this time.

Question 12: When do you expect the accreditation process to begin (i.e., what is the timeframe to be "up and running")?

- Answer: The goal is for the Accreditation Body to be established and prepared to certify candidate C3PAOs in Spring 2020.

Question 13: Are you anticipating more than one accrediting body? If so, do you expect the different organizations to have a specific regional or functional focus?

- Answer: It is anticipated at this time that there will be a single CMMC Accreditation Body that may be comprised of one or more organizations.

Question 14: Will there be any special government contracting requirements other than getting trained/licensed through the future accreditation agency?

- Answer: It is anticipated that C3PAOs will establish a contract / agreement with the Accreditation Body and not the Government.

Question 15: In the RFI there is a reference to, *'Maintain the Reference Implementation Assessment Tool'*, Could you provide some background? Can a proprietary platform/assessment tools could serve the needs of the CMMC Program?

- Answer: The CMMC Accreditation Body will decide the proper use of the assessment tool.

Question 16: What evaluation criteria and weighting factors will be used to select the Accreditation Body?

- Answer: It is anticipated that interested entities will form the Accreditation Body.

Question 17: If a company has specific technical capabilities that they believe will be of value to the Accreditation Body, including the industry community records management systems/databases identified in Section 4.0 of the RFI, should they respond to the RFI describing those capabilities, or should they approach the Accreditation Body directly once it is announced?

- Answer: Please submit a whitepaper in response to the RFI.

Question 18: The user of the term Cybersecurity suggests that privacy controls would be excluded from this pursuit. Does the government intend to address both security and privacy (either alone or in combination as individual certification circumstances dictate) as that is in their best interest?

- Answer: Please refer to the draft CMMC Model (v0.4) on the CMMC website https://www.acq.osd.mil/cmmc/index.html for details of the security requirements and/or practices and processes.

Question 19: Does the scope of this effort pertain solely to CUI? Not suggesting Classified information be included in this program, but there are many other types of data (e.g., FTI, PCI, PHI, PII) that federal entities may have occasion to receive, transmit, or maintain and it would be in the government's best interest to implement a program that would allow organizations to customize their certifications according to the data they have all in one unified but flexible program.

- Answer: Please refer to the draft CMMC Model (v0.4) on the CMMC website https://www.acq.osd.mil/cmmc/index.html for details of what is included within the CMMC Model.

Question 20: The RFI provides a working estimate of 300,000 organizations in the scope of this effort. Could the CMMC Program Office provide a more granular distribution based on size of the organization? If possible it would be helpful if the distribution were not only based on the number of personnel per organization, but also the volume of data each must protect. Additionally, do they intend to have multiple assessments per organization? Such as contractor XYZ who has multiple contract vehicles and possible multiple networks/location? Would this contractor have to undergo multiple assessments?

- Answer: The DIB sector consists of a diverse set of contractors with respect to size, from small to large. The vast majority of the DIB sector consists of small businesses.

Question 21: Does the OUSD anticipate that the CMMC model will be based on or map to FIPS 199 Security Categorizations?

- Answer: The mapping between the CMMC Model and other standards and references will be included in Release version 1.0 in January 2020.

Question 22: Is there a limit to how many entities we can accredit?

- Answer: There is no limit to the number of entities who can receive accreditation. It is anticipated that the number will be driven by the marketplace and the ability of candidate C3PAOs to meet requirements set by the Accreditation Body.

Question 23: Are they modeling this accreditation system after anything else and if so what is that?

- Answer: We are not modeling the accreditation system after any other system. The Accreditation Body may choose to take advantage of lessons learned from other accreditation bodies while meeting requirements.

Question 24: In section one of the program description, it indicates a requirement to submit to the RFI the submitting body should be organized as a "non-profit organization". Is this required to submit content to the RFI and ultimately to be considered as the facilitator or board accreditation body manager if the program is established?

- Answer: For-profit entities can respond to the RFI. Once organized, the Accreditation Body itself will determine its corporate status.

Question 25: Why are only non-profits requested to respond? It should be open to all for information input. It gives the appearance that if the government were to issue a RFP, a level of "pre-selection" is involved.

- Answer: Please see answer associated with Question 1 and Question 24.

Question 26: Preventing loss of Controlled Unclassified Information (CUI) within the Defense Industrial Base (DIB) is critical to maintaining national security is provided as background information in the RFI. If this is so critical, why wouldn't the government provide seed funding, in the event that an RFP is issued, for an organization to work through issues for the first 2-3 years, since the CMMC program is expected to effect at least 300,000 companies or more?

- Answer: Please see answer associated with Question 1.

Question 27: If an RFP is issued and an Accreditation Body is awarded, an MOU may not be the proper mechanism to manage the government's relationship with the Accreditation Body. Has any thought been given to using an Other Transaction Agreement to be flexible to manage the relationship?

- Answer: Please see answer associated with Question 1.

Question 28: SBIR's are important to DOD but are with very small companies, with very few employees. Has there been any thought to work with the SBIR program, to either pay for or guide the company to help with assessment or allow more costs to be added to a phase 1 participant to cover the assessment cost?

- Answer: Any such use of the SBIR program is yet to be determined. Please submit a whitepaper in response to the RFI.

Question 29: I did not see any prohibition for government organizations being accredited. Is this correct?

- Answer: It is anticipated that certified C3PAOs will be commercial, third-party organizations.

Question 30: Once a government contractor is granted a CMMC certification how long is that certification good for?

- Answer: It is anticipated that the Accreditation Body will set the requirements for recertification.

Question 31: Will instructors and/or assessors require clearances for top secret facilities?

- Answer: The certified C3PAOs will only assess non-federal unclassified networks. It is anticipated that the Accreditation Body and/or certified C3PAOs will work with DIB contractors with respect to access requirements for credentialed CMMC assessors.

Question 32: What framework will be used to base the CMMC against?

- Answer: The draft CMMC Model cites multiple references. Please refer to the draft CMMC Model (v0.4) on the CMMC website https://www.acq.osd.mil/cmmc/index.html for details of what is included within the CMMC Model.

Question 33: What are the specific definitions for “micro”, “small” and “mid-sized”?

- Answer: Please refer to the answer associated with Question 20.

Question 34: What is the specific definition for “large” customers?

- Answer: Please refer to the answer associated with Question 20.

Question 35: What are the cut-offs for cybersecurity maturity: low-end, high-end?

- Answer: The draft CMMC Model consists of QTY 5 levels. Please refer to the draft CMMC Model (v0.4) on the CMMC website https://www.acq.osd.mil/cmmc/index.html for details of what is included within the CMMC Model.

Question 36: What is the capacity requirement for training?

- Answer: It is anticipated that the Accreditation Body’s capacity to conduct training will ramp up over time.

Question 37: Will there be any Conflict of Interest restrictions between the Accreditation Body, the C3PAO organizations, and organizations that perform remediation or “security as a service” tasks for DIB vendors?

- Answer: The Accreditation Body will set requirements with respect to conflict of interest amongst these entities.

Question 38: If a company is involved as part of the accreditation body, would they be ineligible to become a C3PAO?

- Answer: Please see the answer associated with Question 37.