REQUEST FOR INFORMATION

CYBERSECURITY MATURITY MODEL CERTIFICATION

ACCREDITATION BODY

OUSD(A&S)

1.0 Description

1.1 The Office of the Undersecretary of Defense (Acquisition & Sustainment) (OUSD(A&S)) in the Department of Defense is seeking information, from ~~non-profit~~ organizations, related to establishment of an Accreditation Body for the Cybersecurity Maturity Model Certification (CMMC) program. The CMMC program will serve as a verification mechanism to ensure appropriate levels of cybersecurity controls and processes are adequate and in place to protect controlled unclassified information (CUI) that resides on the Department's industry partners' networks.

1.2 THIS IS A REQUEST FOR INFORMATION (RFI) ONLY. This RFI is issued solely for information and planning purposes – it does not constitute a Request for Proposal (RFP), nor will it result in an RFP in the future. This request for information does not commit the Government to contract for any supply or service whatsoever. Further, OUSD(A&S) is not at this time seeking proposals and will not accept unsolicited proposals. Respondents are advised that the U.S. Government will not pay for any information or administrative costs incurred in response to this RFI; all costs associated with responding to this RFI will be solely at the interested party's expense. Not responding to this RFI does not preclude participation in any future RFP, if any is issued. If a solicitation is released, it will be synopsized on the Federal Business Opportunities (FedBizOpps) website. It is the responsibility of the potential offerors to monitor these sites for additional information.

2.0 Background

Preventing loss of CUI within the Defense Industrial Base (DIB) is critical to maintaining national security. Existing regulation in the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 and associated clauses requires contractor compliance with certain cybersecurity control standards. The CMMC effort builds upon this existing regulation and combines various cybersecurity control standards (e.g., National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, International Organization for Standardization (ISO) 27001, and Aerospace Industries Association National Aerospace Standards 9933, etc.) into a single, unified standard for cybersecurity. In addition to addressing cybersecurity standards, the CMMC program will use a verification process to assess the maturity of the institutionalization of cybersecurity practices and processes for an organization.

Once implemented, offerors will be required to hold a CMMC certificate at a specified level or higher to be eligible for award on DoD solicitations. To obtain a CMMC certification, companies will coordinate directly with an independent CMMC Third-Party Assessment Organization (C3PAO) that has been accredited by the CMMC Accreditation Body to request and schedule a CMMC assessment. Upon successful demonstration of the appropriate capabilities and organizational maturity, the organization will receive the corresponding CMMC level certification.

The working estimate for the number of organizations requiring CMMC certifications is 300,000, with a very high percentage of those companies in the micro-, small-, and mid-size range. Each assessment will be conducted by a credentialed independent assessor working for an accredited C3PAO under the oversight of the CMMC Accreditation Body.

Definitions and Program Description

CMMC Model – A capability-based maturity model that defines a progression of cybersecurity maturity. The model leverages multiple sources, including current law, regulations, commercial best practices, and threat profiles.

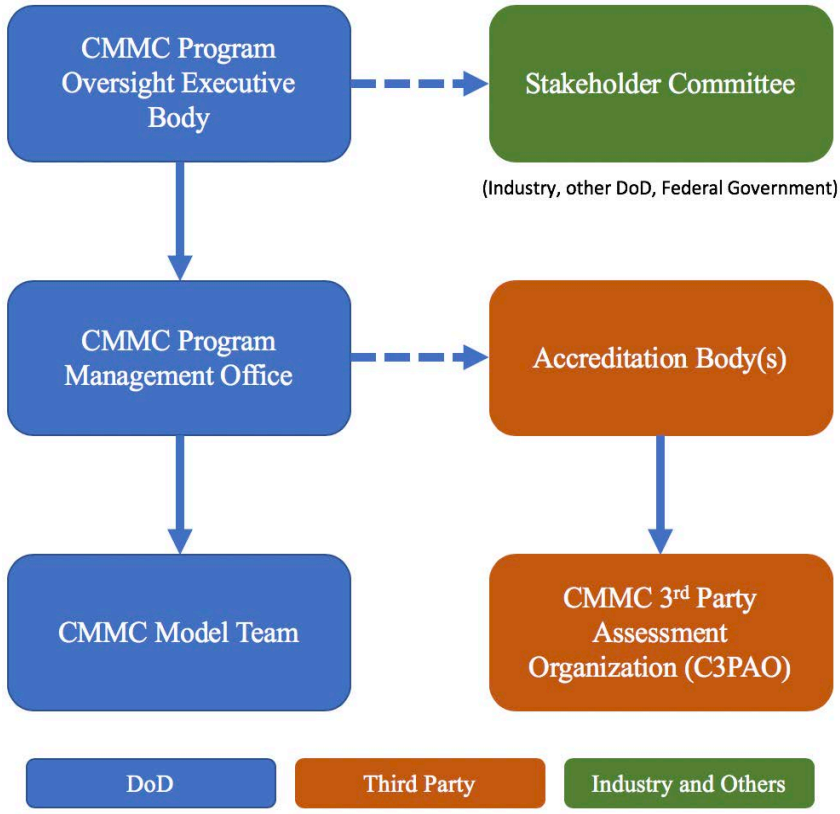
CMMC Accreditation Body – The organization responsible for managing, operating and sustaining the CMMC program, CMMC training, and evaluating and accrediting individual assessors and C3PAOs.

CMMC Assessments – Evidence-based, on-site evaluations of the capabilities, practices, and process maturity defined in the CMMC model and conducted by independent third-party assessment organizations. Not all CMMC assessments will require the same amount of effort, as lower levels defined in the CMMC model assess a smaller number of less challenging cybersecurity capabilities. Higher level assessments will be more involved.

CMMC Certification – The result of a CMMC assessment. The CMMC certification represents a company's demonstration of cybersecurity capabilities and organization maturity as defined for a specific level of the CMMC model. CMMC certification will be used to qualify companies for DoD contracts.

CMMC Third Party Assessment Organizations (C3PAOs) – Third party organizations accredited by the CMMC Accreditation Body and authorized to conduct CMMC assessments and grant CMMC certifications.

The figure below depicts the program relationships among the major components of the CMMC Program.



CMMC Organizational Relationships

3.0 Requested Information

This RFI seeks information on how to define the long-term implementation, functioning, sustainment, and growth of the CMMC Accreditation Body.

The Government's goal is for a non-profit Accreditation Body to complete all activities described in Section 4, Accreditation Body Activities, using revenue generated through dues, fees, partner relationships, conferences, etc. *with no additional funding or resources provided by the Government*. The Government intends that the relationship between the Government and the Accreditation Body will be managed through the use of a Memorandum of Understanding (MOU).

Based on the description of activities described in Section 4, CMMC Accreditation Body Activities, OUSD (A&S) seeks input from industry on the following:

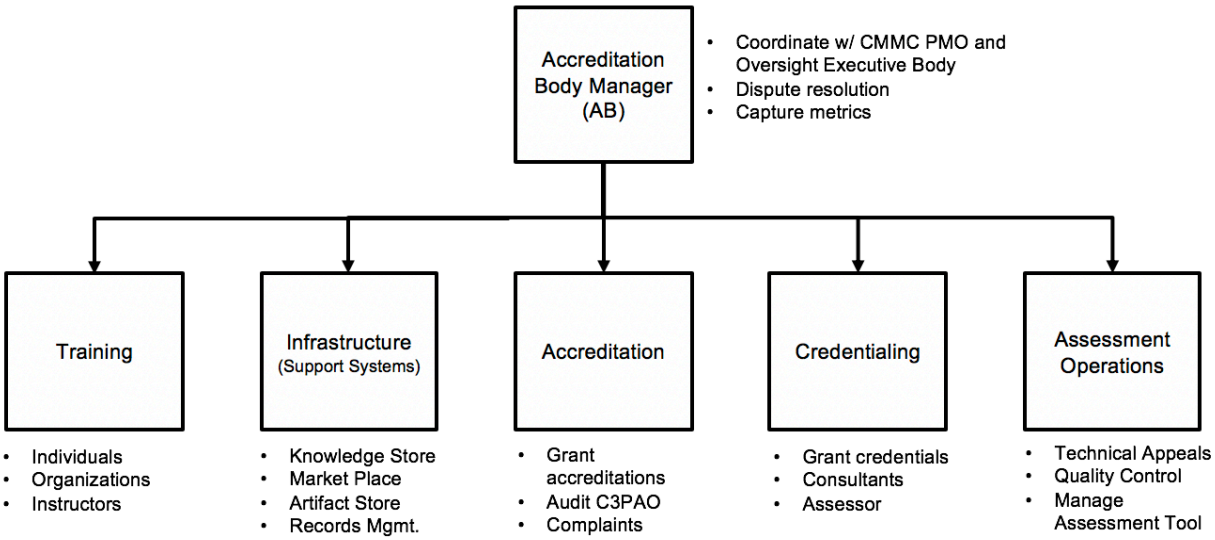
- Description of approaches that meet the Government's intent for the Accreditation Body
- Potential CMMC Accreditation Body organizational structure
- Potential CMMC Accreditation Body financial arrangements (i.e. business model)
- Extent of interest you have in performing one or more of the functions of the Accreditation Body
- Areas where the CMMC Accreditation Body can leverage established organizations, standards, tools, and automation opportunities

4.0 CMMC Accreditation Body Activities

The CMMC Accreditation Body will conduct, but is not limited to, the following ongoing activities:

- Accredit C3PAOs
- Conduct CMMC Training for C3PAOs and Assessors
- Implement individual assessor and C3PAO Quality Control Programs
- Coordinate and report metrics with the CMMC PMO
- Maintain the Reference Implementation Assessment Tool
- Manage and maintain CMMC assessor training, and associated assessment guidance
- Manage and maintain CMMC supporting systems and databases (records management, knowledge sharing and marketplace, artifact store)
- Manage the dispute resolution process to adjudicate C3PAO technical appeals and complaints.

The figure below is a notional functional decomposition that describes potential areas of work associated with the CMMC Accreditation Body activities.



Notional Accreditation Body Functional Decomposition

5.0 Responses

5.1 Interested parties are requested to respond to this RFI with a whitepaper (no minimum criteria for a response). As part of your whitepaper response:

- Describe your organization, relevant experience, and specialized capabilities.
- Address the areas for comment in Section 3 of the RFI.
- Describe how you would potentially accomplish one or all of the above work areas in Section 4 (to include a specified subset of work areas).
- Identify work areas that would be important to operating the CMMC Accreditation Body that are not listed in Section 4.

5.2 White papers in Adobe Acrobat or Microsoft Word for Office compatible format are **due no later than 21 October 2019, 18:00 EST**. Submitted via e-mail to Elizabeth Fuller at elizabeth.e.fuller2.civ@mail.mil.

5.2.1 Proprietary information, if any, should be minimized and MUST BE CLEARLY MARKED. To aid the Government, please segregate proprietary information. Please be advised that all submissions become Government property and will not be returned.

5.3. Section 1 of the white paper shall provide administrative information, and shall include the following as a minimum:

5.3.1. Name, mailing address, overnight delivery address (if different from mailing address), phone number, DUNS/CAGE Code (if available), fax number, and e-mail of designated point of contact.

Company:	Name	Telephone Number	E-mail Address
Company:	Name	Telephone Number	E-mail Address

5.3.2. A statement that the respondent will allow the Government to release its proprietary data to Government support contractors. In the absence of this statement, the Government will assume that the respondent does NOT agree to the release of its submission to Government support contractors.

5.4 Section 2 of the white paper shall be limited to 10 pages and shall *address all topics set forth in Section 5.1* of this RFI. The number of pages in Section 1 of the white paper shall not be included in the 10-page limitation, i.e., the 10-page limitation applies only to Section 2 of the white paper.

6.0 Industry Discussions

OUSD (A&S) representatives may or may not choose to meet with respondents. Such discussions would only be intended to get further clarification of potential capability to meet the requirements, especially any development and certification risks.

7.0 Questions

Questions regarding this announcement shall be submitted in writing by e-mail to the Contracting Officer, Elizabeth Fuller at elizabeth.e.fuller2.civ@mail.mil. Verbal questions will NOT be accepted. Questions will be answered by posting answers to FedBizOpps accordingly, questions shall NOT contain proprietary or classified information. The Government does not guarantee that questions received after **15 October 2019, 18:00 EST** will be answered.

8.0 Summary

THIS IS A REQUEST FOR INFORMATION (RFI) ONLY. The information provided in the RFI is subject to change and is not binding on the Government. OUSD (A&S) has not made a commitment to procure any of the items discussed, and release of this RFI should not be construed as such a commitment or as authorization to incur cost for which reimbursement would be required or sought. All submissions become Government property and will not be returned.