CMMC-AB Continuous Monitoring Request for Proposals

RFP Release Date: 22-April-2020

RFP Response Date: All responses MUST be received no later than 1-May-2020 at 5:00 PM US Eastern Daylight Time

Anticipated Selection: 8-May-2020 by 1:00 PM US Eastern Daylight Time

Contents

Definitions

Accreditation – The process of issuing Licenses and Certificates.

Affiliates - Business concerns, organizations, or individuals that control each other or that are controlled by a common third party. Control may consist of shared management or ownership; common use of facilities, equipment, and employees; or family interest.

Association – The process of linking an Assessor's License Number with the License Number of a C3PAO.

Assessment – The review of an Entity's cybersecurity maturity by an Assessor against the requirements defined in the then-current version of the CMMC. Assessments are performed against a desired CMMC Level.

Assessor – A person who has successfully completed the background, training, and examination requirements as outlined by the CMMC-AB and to whom a License has been issued. Assessors are not CMMC-AB employees.

Audits – The review of a CMMC Certified Entity

Certified 3rd Party Assessment Organization ("C3PAO") – An Entity with which at least two Assessors is Associated and to which a License has been issued.

Certificate – A Record issued to an assessed Entity upon successful completion of an Assessment which evidences the CMMC Level against which the Entity has been successfully assessed.

Certification – The process of receiving a Certificate.

CMMC Certified Entity – An Entity whose cybersecurity program has received a CMMC Certificate from the CMMC-AB.

CMMC – The set of standards initially defined by the DoD against which an Entity is to be Assessed.

Digital Signature – An electronic file which is used to authenticate other electronic files and to encrypt files at rest and/or in motion.

Dispute – A formal process managed by the CMMC-AB through which an Assessor and an Entity being Assessed can seek resolution of a disagreement over the Assessment results.

Dispute Adjudicator – A CMMC-AB employee who is responsible for reviewing and resolving a Dispute.

Educator – CMMC-AB employees who are tasked with educating and testing prospective and current Trainers.

Entity – A legal non-person duly created and maintained under the laws of one or more jurisdiction, including without limitation corporations, limited liability partnerships, and limited liability companies.

License – A document issued to an Assessor, C3PAO, or Trainer, as appropriate, entitling them to perform their duties with respect to the CMMC-AB as further outlined below.

License Number – A unique identified linked to each Assessor, C3PAO, and Trainer.

Record – A physical document, electronic file, entry in an electronic database, or the like.

Trainer – A person Licensed to provide Training to prospective and current Assessors. The Trainers are not CMMC-AB employees.

Background

The United States is under attack. Nation state actors, organized criminal groups, and others are routinely seeking to undermine our citizens' confidence in the government and to steal from our federal, state, and local governments as well as our private corporations and citizens. The United States federal government, and especially the United States Department of Defense ("DoD") is one of the primary targets for many of these attacks. The attackers know that the DoD has strong protections in place, and thus in many cases the attackers begin their attacks farther down the supply chain. The DoD's attempts to encourage those in their supply chain to improve their cybersecurity programs, including implementation of self-certification requirements in its contracts, have not yielded the desired results.

CMMC and the CMMC-AB

DoD created a Cybersecurity Maturity Model Certification ("CMMC") requirement that applies to all organizations in the defense supply chain. A core requirement under CMMC is that a neutral, properly accredited, third party must assess an organization's cybersecurity maturity against criteria defined in the CMMC. This required the creation of an ecosystem around the CMMC, and DoD asked industry to create an Accrediting Body ("CMMC-AB") which is charged with managing the implementation of the CMMC ecosystem and to which the establishment and maintenance of the CMMC standard is chartered. DoD provided the CMMC-AB with version 1.02 of the CMMC model as well as other training materials and assessment guides. As part of the CMMC-AB's efforts to mitigate the risks posed to the country through the sharing of sensitive information with DoD supply chain partners, a continuous monitoring solution will help fill in the gaps between assessments currently scheduled for once every three years. The CMMC-AB is issuing this Request for Proposals ("RFP") to help us identify appropriate partners in our continuous monitoring solution.

CMMC-AB Mission Statement

The CMMC-AB is responsible for the implementation and maintenance of the CMMC ecosystem, including, without limitation, creating educational programs around CMMC, licensing and assessment processes, adjudication, and quality assurance programs. The CMMC-AB's mission will focus on these areas, with the intent of allowing industry to execute many of the related functions.

CMMC-AB Basic Overview

The CMMC-AB will create training programs through which the CMMC-AB can License a cadre of Trainers who will, in turn, train Assessors. The Assessors, upon successful completion of the CMMC-AB's training programs, including associated background checks and examinations, are Licensed to perform formal Assessments under the CMMC. These Assessors will work for Certified Third-Party Assessment Organizations ("C3PAOs"), and these C3PAOs will serve as the interface between the organizations seeking certification ("OSCs"), the Assessment, and the CMMC-AB. OSCs, Assessors and C3PAOs will all utilize the CMMC-AB's continuous monitoring solution to conduct pre-assessment background research as well as monitor companies between formal assessments.

CMMC-AB Geographic Considerations

The CMMC-AB's headquarters site is not yet determined, but the CMMC-AB will likely expand to have a presence in multiple locations throughout the United States. The exact locations are not yet determined, but we believe that the CMMC-AB will have formal points of presence in approximately

nine (9) states/regions, which represent over 61% of the DoD's contracts spending[1]. These states/regions are: California, Washington DC region, Texas, Connecticut, Florida, Washington, Pennsylvania, Massachusetts, and Arizona.

The majority of the C3PAOs and Assessors are anticipated to be located within the United States, but given that DoD maintains bases and other operations in multiple countries, a requirement for assessments is expected in certain key international geographies (e.g., German, Japan, and Korea). A continuous monitoring solution that is deployable on a global scale is therefore advantageous.

Continuous Monitoring Basic Requirements

CMMC-AB intends to augment organizational assessments, which are anticipated to occur at three-year intervals, with continuous monitoring of already-certified DIB organizations to alert for major changes in security posture. The intent is to share early warning of issues with DIB organizations and alert them to externally visible vulnerabilities. The addition of an installed agent or device is not currently contemplated, and the CMMC-AB will not consider such solutions in response to this RFP.

The CMMC-AB seeks external information and assistance in the development of associated continuous monitoring activities. This RFP is NOT for a general portal or website for use by the AB. This continuous monitoring solution should incorporate the following basic activities:

1. Non-intrusive (Not a Penetration Test) review and analysis of company internet traffic on the public domain.
2. Analysis of traffic that is on the public domain only.

A list of potential activities that the CMMC-AB wishes to contract is below. This list is not exhaustive and may change up to the point of contract signing.

1. Acceptance and securing of AB and DOD intellectual property.
2. Create a secure portal specifically for the containment, use and display of continuous monitoring security related data, including possible multifactor access that supports the DoD's Common Access Card ("CAC"), for the following stakeholders:
    a. OSCs – A self-service dashboard that shows individual companies their own security posture as assessed by the continuous monitoring solution, including listing all security activities, scores, and other metrics for their company.
    b. Authorized DoD Staff –Read-only access and that allows the staffer to search for and view information on any company in the database and to access aggregated metrics from across all monitored companies and defined subsets thereof (e.g., manufacturing companies, technology services companies, landscaping companies, etc.).
    c. Authorized CMMC-AB Staff – normal administrative and non-admin functions. Full permissions for admin and less (read, write) for non-admin staff. CMMC-AB staff should also receive automatic notifications when any company has a security score decrease a specific amount.

[1] See page 6 of http://www.oea.gov/sites/default/files/fy2017-r2/FY2017_Defense_Spending_by_State_Report_Web_Version_20190315.pdf

d. C3PAOs and/or Assessors – In their preparation for an assessment, C3PAOs and/or Assessors should be able to log into a company's dashboard to review the current state of that company's security posture as it is being monitored. In addition, C3PAO's and/or Assessors should also be able to receive automatic notifications when any company they were responsible for assessing has a security score decrease a specific amount. The amount will be TBD.

3. Once the CMMC-AB has built its web application for managing assessments, training, certification and licenses, this solution should have an API or other mechanism for transmitted data, dashboards, and/or reports to it.
4. Provides automated methods for prioritizing findings and issues.
5. Provides issue severity information for the findings provided.
6. Provides asset value information for the findings provided.
7. Ability to filter findings based on an organization's specific risk policies.

The CMMC-AB and the DoD will address this critical aspect of national security via the CMMC program. We are therefore asking potential external continuing monitoring partners who are interested in serving as the continuous monitoring solution to the CMMC-AB to respond to this Request for Proposals no later than the date and time indicated on the coversheet of this RFP with the following information:

1) A brief overview of their company's capabilities with respect to our needs as outlined above.
1) Team biographies and expertise specific to our needs.
2) Representative experience (client lists, case studies, references and the like).
3) The company's approach to client service, client satisfaction, and feedback, including:
    a. The company's plan for learning more about the CMMC and the CMMC-AB, the surrounding industry, etc.;
    b. The training the company can provide to the CMMC-AB's board of directors and senior executives;
    c. The company's approach to risk identification and risk management, both internally and for clients;
    d. The company's approach to quality assurance for its work.
    e. The breadth of experience across the company, which will help us understand the company's ability to respond quickly to larger tasks and/or when a primary point of contact at the firm is unavailable.
4) The company's proposed fee structure, including estimated fees for:
    a. The creation of the continuous monitoring solution
    b. The creation of secure portal for accessing information
    c. All documentation
    d. Initial and recurring training on the systems
    e. Initial (non-binding) licensing terms
5) List any cybersecurity standards against which the company's information technology systems has been certified and indicate whether those are self-certifications or third-party certifications (and provide the name of the third party).
6) A short set of business advice you suggest similarly situated organizations follow.
7) A description of what we will lose if we do not select your firm.

8) Any other information that you feel would be advantageous for the CMMC-AB to understand in making its decision.

Questions for the CMMC-AB

Chris Golden is the primary point of contact for this effort. Please direct any questions to him at cgolden@cmmcab.org, and he will coordinate a response from the CMMC-AB.

Proposal Submissions

Send proposals to cgolden@cmmcab.org no later than the date indicated on the cover page of this RFP.