

---

## **Memorandum of Understanding**

---

between

**The Department of Defense,  
Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))  
and  
Cybersecurity Maturity Model Certification Accreditation Body, Inc. (CMMC-AB)**

### **I. Purpose:**

This Memorandum of Understanding (MOU) sets forth the understandings held by both the Department of Defense (DoD or Department) and the Cybersecurity Maturity Model Certification Accreditation Body, Inc. (CMMC-AB) regarding Cybersecurity Maturity Model Certification (CMMC) accreditation, certification, approval, training and assessment processes as related to the Defense Supply Chain (DSC). The DoD and CMMC-AB are collectively referred to herein as the "parties".

### **II. Acceptance of CMMC Certifications**

CMMC-AB is responsible for and authorized to manage, control, and administer CMMC assessment, certification, training, and accreditation processes with respect to the DSC. DoD intends to utilize the results of the CMMC-AB's accreditation efforts to satisfy future DoD solicitation requirements regarding an entity's CMMC certification status.

The Department of Defense will accept only CMMC certifications issued by an assessor who has been accredited to perform CMMC assessments by an Accreditation Body or a CMMC Third Party Assessment Organization (C3PAO) accredited by that same Accreditation Body. The Accreditation Body must be accepted and recognized by the DoD pursuant to a signed Memorandum of Understanding (MOU) or a DoD contract. Any other CMMC certifications are invalid and will not be acceptable to satisfy future DoD solicitation requirements regarding an entity's CMMC certification status.

### **III. Background:**

The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) recognizes that security is foundational to acquisition and should not be diminished in favor of cost, schedule, or performance. Therefore, OUSD(A&S) is committed to working with the defense supply chain (DSC) to enhance the protection of federal contract information and Controlled Unclassified Information (CUI) within the DSC. To further this effort, OUSD(A&S) has worked with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDCs), and industry to develop the CMMC Model.

The CMMC Model combines various cybersecurity standards and best practices and maps the resulting controls and processes across several maturity levels that range from basic to advanced cyber hygiene. For a given CMMC level, the associated controls and processes, when implemented, will reduce risk against a specific set of cyber threats. The CMMC effort builds upon existing regulatory efforts that are based on trust by adding a verification component with respect to cybersecurity requirements.

Cybersecurity of the DSC is critical to the successful execution of DoD's mission. Through its day-to-day management and oversight of the processes associated with the implementation and operations of the CMMC, the CMMC-AB will play an instrumental role in helping the Department achieve its goal of improving the DSC's cybersecurity posture.

#### **IV. General Provisions**

This MOU represents the broad outline of the parties intention to collaborate in areas of mutual interest with the following provisions:

1. This MOU is not a contract and does not create legally enforceable duties or obligations for either party. This MOU only sets forth the understandings of the parties with respect to the purpose stated in Section. I.
2. Any action that either party chooses to take in relation to the understandings set forth in this MOU is subject to the availability of personnel, resources, and funds.
3. This MOU does not affect or supersede any existing or future understandings or arrangements between the parties and does not affect the ability of the parties to enter into other understandings or arrangements related to this MOU.
4. This MOU and any actions taken by the parties in connection with or in furtherance of the purpose of this MOU are subject to any applicable policies, rules, regulations, and statutes under which DoD and the CMMC-AB operate.

#### **V. CMMC-AB Functions:**

The CMMC-AB operates as an independent accreditation entity that manages and oversees CMMC accreditation, certification, approval, training, and assessment processes including, but not limited to, the below-listed items:

1. Develop, maintain, keep current, validate, and protect the "CMMC Standard," which consists of the criteria or requirements used by the CMMC-AB to certify individuals and accredit entities, as well as all associated research, validation, training, assessing, measuring, testing, or other materials or information, including forms, systems, processes, procedures, platforms, and software, all according to, and consistent with, the CMMC Model provided by the DoD CMMC Program Management Office (PMO).

2. Administer applications from organizations requesting certification as CMMC Third Party Assessment Organizations (C3PAOs).
3. Administer applications from individuals requesting certification as CMMC assessors.
4. Administer applications from individuals requesting approval as CMMC trainers.
5. Certify contractors in the DSC at the identified levels of cybersecurity maturity established in the CMMC model.
6. Develop, maintain, and provide training, including curricula and testing, for trainers, individual assessors, and, as necessary, C3PAOs.
7. Develop, maintain, manage, and secure a database(s) to track certification, approval, and training requirements and status for C3PAOs, assessors, and trainers.
8. Develop, maintain, manage, and secure a separate database for CMMC Assessment Reports.
9. Establish, maintain, and manage an up-to-date list of certified C3PAOs on a publicly-accessible CMMC "Marketplace" website whose specific name and detailed function will be mutually agreed upon by the parties.
10. Implement a transparent and equitable dispute resolution process with respect to both technical and ethical issues regarding training and CMMC assessments.
11. Implement a quality assurance program with respect to training and CMMC assessments.

## **VI. Activities and Operations:**

### **DoD:**

The CMMC-AB understands that the DoD will conduct the following activities described below:

1. Establish and maintain a CMMC PMO.
2. Retain sole responsibility for maintaining and updating the CMMC Model and Assessment Guides to incorporate changes in cybersecurity requirements and threats.
3. Provide CMMC Model, CMMC Assessment Guides, and all updates to the CMMC Model and CMMC Assessment Guides to the CMMC-AB.
4. Provide the CMMC-AB with initial draft training material on CMMC background information, the CMMC Model, and CMMC Assessment Guides to inform and

shape the training curriculum and associated materials for which the CMMC-AB is ultimately responsible.

5. Establish and maintain the CMMC Certification Database infrastructure.
6. Communicate the requirement to achieve CMMC certification to companies in the DSC.
7. Provide factual information to the CMMC-AB as reasonably requested in connection with the CMMC-AB's efforts to secure private sector funding for the initial operation of the CMMC-AB.
8. Provide factual information to the CMMC-AB as reasonably requested in connection with the CMMC-AB's application to the Internal Revenue Service for a tax exemption determination that CMMC-AB is an organization described in Internal Revenue Code Section 501(c)(3).
9. Provide to the CMMC-AB the appropriate federal points of contact and available resources to enable the CMMC-AB to properly direct questions received regarding small business issues.
10. Provide subject matter expertise regarding the CMMC Model in support of CMMC-AB activities, including development of training materials.
11. Provide information to the CMMC-AB as reasonably requested in connection with the CMMC-AB's efforts to obtain security authorizations. To the extent authorized by law, regulation, and policy, provide assistance and prioritization for CMMC-AB personnel in obtaining security clearances as required for performance of CMMC-AB operations with respect to the DSC. Provide security authorization of CMMC-AB infrastructure, including networks, encryption, identity management or other capabilities as needed.
12. Protect proprietary CMMC-AB intellectual property, including patents, trademarks, copyrights, and trade secrets, to the extent required by law.
13. Establish and maintain appropriate and consistent communication channels with the CMMC-AB regarding all CMMC-AB efforts as related to the DSC and facilitate PMO sessions with the CMMC-AB throughout the duration of this MOU.
14. To the extent authorized by law and in compliance with applicable DoD policies, share critical cyber threat information with the CMMC-AB to support modifications to its operational procedures and mission assurance.
15. Conduct a PMO-led annual review to determine the parties' alignment with the understandings set forth in this MOU.

**Accreditation Body:**

DoD understands that the CMMC-AB will conduct the following activities described below:

1. Maintain self-sustaining, independent CMMC accreditation operations with no funding provided by the DoD.
2. Achieve and maintain the current International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 17020 certification.
3. Achieve and maintain the current ISO / IEC 17011 certification.
4. Establish and maintain the CMMC Standard and all associated training, credentialing, and accreditation requirements, processes, and materials in accordance with the CMMC Model provided by the DoD CMMC Program Management Office (PMO).
5. Require leadership and internal staff, to include Information Technology (IT) staff, to be U.S. Citizens and undergo a background check consistent with a National Agency Check (NAC), DHS Suitability, or other DoD-accepted security clearance methods.
6. Require all outsourced IT or Managed Service Providers (MSP) support organizations to undergo a background check consistent with a NAC or DHS Suitability, or DOD security clearance as required.
7. Require all internal IT systems and/or networks to be equivalent CMMC Level 3 certified by government assessors from the Defense Contracting Management Agency (DCMA).
8. Require all outsourced IT and/or MSP support organizations to be equivalent CMMC Level 3 certified by government assessors from the DCMA within two years of the date of this MOU.
9. If the CMMC-AB utilizes a commercial cloud service, the commercial cloud service provider shall meet or exceed the equivalent of the FedRAMP Moderate baseline, for any cloud applications used as a part of the delivery of accreditation and certification services.
10. Approve CMMC certificates for DSC contractors and upload CMMC certificates to the CMMC Certification Database.
11. Provide access to CMMC Certification Database for CMMC-AB users, provided that the Government must approve and authenticate any such user and may deny access in its sole discretion.

12. Collaborate with DoD PMO to aid in the Department's efforts to assess potential supply chain risk with respect to national security concerns.
13. Require that all candidate C3PAO's achieve and maintain the current ISO/IEC 17020 certification as a condition to accreditation as a C3PAO for level 3 and above assessments.
14. Enable certified assessors employed by certified C3PAOs to conduct assessments and inform risk.
15. Establish policies and procedures for reciprocity to take into consideration the results of other assessments performed on the entity requesting accreditation, e.g. ISO, FedRamp, DoD Assessment.
16. Provide consistent and accurate monthly status update reports to the CMMC PMO, to include significant findings and C3PAO accreditation status.
17. Participate in an annual review held by the CMMC PMO to determine adherence to the parties' responsibilities as defined in this MOU.
18. Establish and maintain appropriate and consistent communication channels with the CMMC-AB regarding all CMMC-AB efforts as related to the DSC and facilitate PMO sessions with the CMMC-AB throughout the duration of this MOU.
19. Establish and maintain policies and procedures that evaluate and incorporate feedback from the CMMC PMO to improve the Accreditation Body's CMMC accreditation processes.

## **VII. Duration, Termination and Survival.**

This MOU shall become effective upon signature by the authorized officials from the CMMC-AB and DoD and will remain in effect until modified by mutual consent, or terminated by either party. The parties may review this MOU on an annual basis or as needed, and the MOU may be modified by mutual consent of authorized officials from DoD and the CMMC-AB. Both parties will make best efforts to provide reasonable advance notice of pending changes to the MOU with highly significant or major impact to the CMMC program.

Both parties acknowledge that leadership or other changes have potential ramifications with respect to the understandings set forth in this MOU. Should the need for this MOU change, both parties will provide reasonable advance notice to the other party and work in good faith to modify the MOU to address the changes prior to termination.

Either party may raise concerns regarding the other party's actions in connection with this MOU. Both parties will work to resolve any issues or differences in a good faith and expedient manner prior to terminating the MOU.

**VIII. Return of Proprietary Information.**

Upon termination, and absent mutual agreement to alternative procedures, the parties will cease all use of information identified as or otherwise constituting the other party's proprietary information received hereunder and return or, as agreed, certify destruction of all such information received from the other party including all copies thereof. Recipients may retain one archival copy.

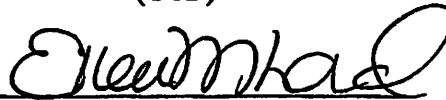
**IX. Points of Contact.** Points of contact for this MOU are:

<b>DoD</b> 3010 Defense Pentagon Washington, DC 20310 Attention: Ellen M. Lord Phone: (703) 697-7021 E-mail: ellen.m.lord.civ@mail.mil	<b>CMMC-AB</b> 936 Fell Street Baltimore, MD, 21231 Attention: Ty A. Schieber Phone: (540) 220-1099 E-mail: tschieber@cmmcab.org
---	---

**X. Endorsing Signatures.** This MOU is hereby endorsed by our hand:

(OSD)

CMMC-AB

By:   
Signature

By:   
Signature

Name: The Honorable Ellen M. Lord

Name: Ty A. Schieber

Title: USD(A&S)

Title: Board Chairman, CMMC-AB

Date: 17 Mar 2020

Date: 23 MAR 2020