SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, AND 30

1. REQUISITION NUMBER

PAGE 1 OF 39

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
HQ003420H0003P00001	25-Nov-2020			

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER *(No Collect Calls)*	8. OFFER DUE DATE/LOCAL TIME

9. ISSUED BY CODE HQ0034

WHS - ACQUISITION DIRECTORATE
4800 MARK CENTER DRIVE, SUITE 09F09
ALEXANDRIA VA 22350

TEL:
FAX:

10. THIS ACQUISITION IS [X] UNRESTRICTED OR [ ] SET ASIDE: _____ % FOR:

- [ ] SMALL BUSINESS
- [ ] WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- [ ] HUBZONE SMALL BUSINESS
- [ ] EDWOSB
- [ ] SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- [ ] 8(A)

NAICS: 813920

SIZE STANDARD: $16,500,000

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED
[ ] SEE SCHEDULE

12. DISCOUNT TERMS

[ ] 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION
[ ] RFQ [ ] IFB [ ] RFP

15. DELIVER TO CODE HQ0157

OUSD(A&S) OCISO
(b)(6)
4800 MARK CENTER
ALEXANDRIA VA 22350-3400

16. ADMINISTERED BY CODE

SEE ITEM 9

17a. CONTRACTOR/ OFFEROR CODE 8HGJ5 FACILITY CODE 8HGJ5

CYBERSECURITY MATURITY MODEL CERTIFICATI
(b)(6)
936 FELL ST
BALTIMORE MD 21231-3504

TELEPHONE NO (b)(6)

18a. PAYMENT WILL BE MADE BY CODE

[ ] 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a. UNLESS BLOCK BELOW IS CHECKED [ ] SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/ SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	SEE SCHEDULE				

25. ACCOUNTING AND APPROPRIATION DATA

26. TOTAL AWARD AMOUNT (For Govt. Use Only)
$0.00

[ ] 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1. 52.212-4. FAR 52.212-3. 52.212-5 ARE ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

[ ] 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA [ ] ARE [ ] ARE NOT ATTACHED

[ ] 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 0 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED.

[ ] 29. AWARD OF CONTRACT: REF. OFFER DATED . YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)
(b)(6)

30b. NAME AND TITLE OF SIGNER *(TYPE OR PRINT)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(TYPE OR PRINT)*	31c. DATE SIGNED
		(b)(6) / Contracting Officer (b)(6) EMAIL: (b)(6)	25-Nov-2020

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 2/2012)
Prescribed by GSA – FAR (48 CFR) 53.212

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS (CONTINUED)					PAGE 2 OF 39
19. ITEM NO.	20. SCHEDULE OF SUPPLIES/ SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	SEE SCHEDULE				

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
	32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER ☐ PARTIAL ☐ FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT ☐ COMPLETE ☐ PARTIAL ☐ FINAL	37. CHECK NUMBER

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

HQ003420H0003

Section SF 1449 - CONTINUATION SHEET

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001		1	Lot	$0.00	$0.00

CMMC AB Services
FFP
Cybersecurity Maturity Model Certification (CMMC) Accreditation Body (AB) Services
Perform services in accordance with the attached Statement of Work (SOW) and Terms and Conditions (T&Cs).

FOB: Destination
R799

NET AMT $0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
1001		1	Lot	$0.00	$0.00
OPTION					

CMMC AB Services
FFP
Cybersecurity Maturity Model Certification (CMMC) Accreditation Body (AB) Services
Perform services in accordance with the attached Statement of Work (SOW) and Terms and Conditions (T&Cs).

FOB: Destination
R799

NET AMT $0.00

HQ003420H0003

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
2001		1	Lot	$0.00	$0.00
OPTION	CMMC AB Services FFP Cybersecurity Maturity Model Certification (CMMC) Accreditation Body (AB) Services Perform services in accordance with the attached Statement of Work (SOW) and Terms and Conditions (T&Cs). FOB: Destination R799				
				NET AMT	$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
3001		1	Lot	$0.00	$0.00
OPTION	CMMC AB Services FFP Cybersecurity Maturity Model Certification (CMMC) Accreditation Body (AB) Services Perform services in accordance with the attached Statement of Work (SOW) and Terms and Conditions (T&Cs). FOB: Destination R799				
				NET AMT	$0.00

HQ003420H0003

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
4001		1	Lot	$0.00	$0.00
OPTION	CMMC AB Services FFP Cybersecurity Maturity Model Certification (CMMC) Accreditation Body (AB) Services Perform services in accordance with the attached Statement of Work (SOW) and Terms and Conditions (T&Cs). FOB: Destination R799				
				NET AMT	$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
5001		1	Lot	$0.00	$0.00
OPTION	CMMC AB Services FFP Cybersecurity Maturity Model Certification (CMMC) Accreditation Body (AB) Services Perform services in accordance with the attached Statement of Work (SOW) and Terms and Conditions (T&Cs). FOB: Destination R799				
				NET AMT	$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
6001		1	Lot	$0.00	$0.00
OPTION	CMMC AB Services FFP Cybersecurity Maturity Model Certification (CMMC) Accreditation Body (AB) Services Perform services in accordance with the attached Statement of Work (SOW) and Terms and Conditions (T&Cs). FOB: Destination R799				
				NET AMT	$0.00

ITEM NO	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
7001		1	Lot	$0.00	$0.00
OPTION	CMMC AB Services FFP Cybersecurity Maturity Model Certification (CMMC) Accreditation Body (AB) Services Perform services in accordance with the attached Statement of Work (SOW) and Terms and Conditions (T&Cs). FOB: Destination R799				
				NET AMT	$0.00

This agreement is entered into this 25 day of November 2020, by the United States of America (the “Government”) represented by Elizabeth Fuller, the Contracting Officer, and Cybersecurity Maturity Model Certification – Accreditation Body, Inc. (CMMC-AB), a corporation organized and existing under the laws of the State of Virginia (the “Contractor”).

INSPECTION AND ACCEPTANCE TERMS

Supplies/services will be inspected/accepted at:

CLIN	INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
0001	Destination	Government	Destination	Government
1001	Destination	Government	Destination	Government
2001	Destination	Government	Destination	Government
3001	Destination	Government	Destination	Government
4001	Destination	Government	Destination	Government
5001	Destination	Government	Destination	Government
6001	Destination	Government	Destination	Government
7001	Destination	Government	Destination	Government

DELIVERY INFORMATION

CLIN	DELIVERY DATE	QUANTITY	SHIP TO ADDRESS	DODAAC / CAGE
0001	POP 25-NOV-2020 TO 24-NOV-2023	N/A	OUSD(A&S) OCISO (b)(6) 4800 MARK CENTER ALEXANDRIA VA 22350-3400 (b)(6) FOB: Destination	HQ0157
1001	POP 25-NOV-2023 TO 24-NOV-2024	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0157
2001	POP 25-NOV-2024 TO 24-NOV-2025	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0157
3001	POP 25-NOV-2025 TO 24-NOV-2026	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0157
4001	POP 25-NOV-2026 TO 24-NOV-2027	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0157
5001	POP 25-NOV-2027 TO 24-NOV-2028	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0157
6001	POP 25-NOV-2028 TO 24-NOV-2029	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0157
7001	POP 25-NOV-2029 TO 24-NOV-2030	N/A	(SAME AS PREVIOUS LOCATION) FOB: Destination	HQ0157

CLAUSES INCORPORATED BY FULL TEXT

52.204-25 PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020)

(a) Definitions. As used in this clause--

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means--

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means--

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled--

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition.

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) Exceptions. This clause does not prohibit contractors from providing--

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.

(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause:

(i) Within one business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: Any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

52.217-8 OPTION TO EXTEND SERVICES (NOV 1999)

The Government may require continued performance of any services within the limits specified in the contract. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 60 days prior to contract expiration.

(End of clause)

52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor at any time prior to the expiration of the contract; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 10 years and six months.

(End of clause)

WHS/AD LOCAL CLAUSE: CONTRACTING OFFICER'S REPRESENTATIVE (COR) (MAR 2015)

(a) The Contracting Officer's Representative (COR) is a representative of the Government with limited authority who has been designated in writing by the Contracting Officer to provide technical direction, clarification, and guidance with respect to existing specifications and performance work statement/statement of work/statement of objectives, as established in the contract. The COR also monitors the progress and quality of the Contractor's performance for payment purposes. The COR shall promptly report Contractor performance discrepancies and suggested corrective actions to the Contracting Officer for resolution.

(b) The COR is not authorized to take any direct or indirect actions or make any commitments that will result in changes to price, quantity, quality, schedule, place of performance, delivery or any other terms or conditions of the written contract.

(c) The Contractor is responsible for promptly providing written notification to the Contracting Officer if it believes the COR has requested or directed any change to the existing contract. No action shall be taken by the Contractor for any proposed change to the existing contract. No action shall be taken by the Contractor for any proposed change to the contract until the Contracting Officer has issued a written directive or a written modification to the contract. The Government will not accept and is not liable for any alleged change to the contract unless the change is included in a written contract modification or directive signed by the Contracting Officer.

(d) COR authority is not delegable.

(e) The COR for this contract is:

(b)(6)
CMMC Director
OUSD(A&S)/OCISO
Email: (b)(6)

(end of clause)

Exhibit/Attachment Table of Contents

DOCUMENT TYPE	DESCRIPTION	PAGES	DATE
Attachment 1	DD254 Revision 1	4	07-APR-2021
Attachment 2	Risk Matrix	4	23-NOV-2020

STATEMENT OF WORK

The Cybersecurity Maturity Model Certification Accreditation Body
Statement of Work (SOW)

I. Purpose:

The Department of Defense (DoD) will use the Cybersecurity Maturity Model Certification – Accreditation Body, Inc. (CMMC-AB), a non-profit organization, as the authoritative source to accredit CMMC Third Party Assessment Organizations (C3PAOs) and the CMMC Assessors and Instructors Certification Organization (CAICO). The DoD will retain oversight of the CMMC program and will be responsible for establishing CMMC assessment and training requirements as well as developing, updating, maintaining, and publishing the CMMC Model, all CMMC Assessment Guides, and policies for the DoD implementation of the CMMC framework.

II. 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. OUSD(A&S) is committed to working with the Defense Industrial Base (DIB) sector to enhance the protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within the supply chain. 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, which is available at https://www.acq.osd.mil/cmmc/.

The CMMC Model combines various standards, references, and best practices into a unified standard. The model aligns sets of cybersecurity practices and maturity processes with the sensitivity of information to be protected and the associated threats. The CMMC framework builds upon existing regulations and efforts by adding a verification component and assessing the implementation of cybersecurity requirements.
The CMMC-AB shall accredit C3PAOs and the CAICO in accordance with International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) standards. Through these activities, the CMMC-AB will be instrumental to the Department achieving its goal of improving the DIB sector's cybersecurity posture.

III. General Provisions:

1. This is a no cost contract. CMMC-AB shall provide all services as required by the contract at no direct cost or "gratuitously" to the Government. The Government shall not be liable for any payment arising under the contract.
2. This agreement does not impact future understandings or arrangements between the parties and does not affect the ability of the parties to enter into other understandings or arrangements with each other related to this no cost contract or any subsequent amendments.
3. The DoD grants the right to the CMMC-AB to serve as the exclusive accreditation body to support the execution of CMMC in accordance with DoD policies and requirements to include the CMMC Model and CMMC Assessment Guides.
4. The CMMC-AB shall achieve compliance with the current ISO/IEC 17011 standard no later than 31 October 2022. The CMMC-AB shall complete the peer assessment of conformity in accordance with the ISO Committee on Conformity Assessment (CASCO) and demonstrate compliance with all ISO/IEC 17011 requirements no later than 31 October 2022.
    a. The CMMC-AB, upon achieving ISO/IEC 17011 compliance, shall maintain compliance with the ISO/IEC 17011 standard to include meeting all requirements for self-assessments, peer reviews, and other assessments.
    b. The CMMC-AB shall become a full member of InterAmerican Accreditation Cooperation (IAAC) after achieving ISO/IEC 17011 compliance and shall remain in good standing.
5. During the two year period starting 31 October 2020 and ending 30 October 2022, the CMMC-AB shall achieve ISO/IEC 17011 compliance through the appropriate peer review process. The CMMC-AB shall:
    a. Become an associate member of the InterAmerican Accreditation Cooperation (IAAC) and remain in good standing.
    b. Develop and update a comprehensive plan and schedule to comply with all ISO/IEC 17011 requirements. As part of this plan, include a detailed risk mitigation plan for all potential conflicts of interest that may pose a risk to compliance with ISO/IEC 17011.
    c. Develop, maintain, and provide provisional training, including curricula and testing, for instructors and individual assessors. The CMMC-AB shall coordinate all provisional training and testing content with the OUSD(A&S)/OCISO(A&S) CMMC Office for review prior to implementation to ensure compliance with the CMMC Model, CMMC Assessment Guides and DoD policies and, to verify conformance with the Government requirements specification. The Government specification is subject to change control procedures that include, but are not limited to, impact, schedule, and risk analysis. The

outcome of the change control procedures will be mutually agreed upon with the Government.

d. Ensure the quality control of all training products, instruction, and testing to include reviews with respect to cybersecurity technical accuracy and alignment with the CMMC Model, CMMC Assessment Guides, and DoD cybersecurity requirements and policies.
e. Develop, maintain, and manage database(s) to track the status of all authorized and accredited C3PAOs, provisional assessors, trainers and instructors. All data shall be replicated and backed up daily to CMMC eMASS or an alternative DoD system.
f. The CMMC-AB shall provide documentation showing the CMMC-AB's current ecosystem, which includes but is not limited to C3PAOs, the CAICO, Assessors, Registered Provider Organizations, Registered Practitioners, Licensed Instructors, Licensed Partner Publisher, and Licensed Training Providers. These shall be in strict compliance with the specified DoD requirements referred to in Section III(6) below. The CMMC-AB shall provide the OUSD(A&S)/OCISO(A&S) CMMC Office with all plans and/or changes related to CMMC-AB activities and the CMMC ecosystem to review prior to implementation and publication.

6. The CMMC-AB shall develop and maintain a quality assurance program with respect to the accreditation of C3PAOs and the CAICO in accordance with ISO/IEC 17011 and specified DoD requirements to be provided to the CMMC-AB NLT 31 January 2021 via a bilateral modification and incorporation in the contract IAW Article III.B of the terms and conditions.
7. The CMMC-AB shall provide all plans that are related to potential sources of revenue to include but not limited to fees, licensing, membership, and/or partnerships to the OUSD(A&S)/OCISO(A&S) CMMC Office. The OUSD(A&S)/OCISO(A&S) CMMC Office must acknowledge receipt and provide suggested guidance for compliance prior to the CMMC-AB implementing and publicizing.
8. The CMMC-AB Board of Directors, professional staff, Information Technology (IT) staff, accreditation staff, and contracted independent assessor staff shall be U.S. citizens shall achieve a favorably adjudicated Tier 3 suitability determination.
9. The OUSD(A&S)/OCISO(A&S) CMMC Office has the responsibility to establish the requirements for CMMC assessment and training certifications and the accreditation requirements for C3PAOs and the CAICO. OUSD(A&S)/OCISO(A&S) CMMC Office will also develop, update, maintain, and publish the CMMC Model and all CMMC Assessment Guides. The CMMC Model contains the cybersecurity requirements by which all DIB companies will be assessed against. The CMMC Assessment Guides shall serve as the singular authoritative reference for the conduct of assessments and associated activities to be used by DIB contractors, C3PAOs, assessors, training organizations and instructors, and the CMMC-AB.
10. The OUSD(A&S)/OCISO(A&S) CMMC Office shall establish and maintain the single DoD database or an alternative DoD system, to store and process assessment related data elements and the associated assessment reports. The OUSD(A&S)/OCISO(A&S) CMMC Office will provide C3PAOs and the CMMC-AB the appropriate access to perform their respective functions.

IV. CMMC-AB Duties:

A. Authorization and Accreditation of C3PAOs

1. Authorize C3PAOs to conduct CMMC assessments, during the 24-month period starting 31 October 2020 and ending 30 October 2022. Prior to authorizing any C3PAO to conduct CMCC assessments, the CMMC-AB shall verify that the C3PAO has met all specified DoD requirements (to be provided to the CMMC-AB NLT 31 January 2021 via a bilateral

modification and incorporation in the contract IAW Article III.B of the terms and conditions) with the exception of achieving the ISO/IEC 17020 accreditation requirements.
    - C3PAOs shall not be authorized to conduct CMMC assessments until achieving CMMC Level 3 certification themselves for their unclassified networks and/or segments (internal and external) that store, process, and transmit CUI.
    - Require that all C3PAOs authorized to conduct CMMC assessments be subjected to quality assurance reviews to include but not limited to observations of their conduct and management of CMMC assessment processes.
2. Accredit C3PAOs in accordance with ISO/IEC 17020 and DoD requirements.
    - Require all C3PAOs achieve and maintain the ISO/IEC 17020 accreditation requirements within 27 months of registration.
3. Require C3PAOs to electronically submit pre-assessment material, final assessment reports and appropriate CMMC certificates to OUSD(A&S)/OCISO(A&S) CMMC Office via CMMC eMASS or an alternative DoD system.
4. The CMMC-AB will provide an up-to-date list of registered candidate C3PAOs, authorization and accreditation records and status. This data will include the dates associated with the authorization and accreditation of each C3PAO. This information will be stored by the DoD in the CMMC eMASS or an alternative DoD system, using the format specified by the DoD.
5. Require C3PAOs to establish a formal process to address DIB contractor complaints and appeals, in accordance with ISO/IEC 17020, and submit investigation and decisions, to include dispute resolution results, to OUSD(A&S)/OCISO(A&S) CMMC Office via CMMC eMASS.
6. Require the C3PAO to agree that if it loses authorization or accreditation, that it must return or provide certification that it has destroyed all assessment related records in its possession.
7. Establish, maintain, and manage an up-to-date list of authorized and accredited C3PAOs on a publicly-accessible CMMC “Marketplace” website whose specific name and detailed function will be mutually agreed upon by the parties. The CMMC-AB shall provide a listing of these entities and their status to the DoD.
8. The CMMC-AB shall not publish nor change requirements for the authorization and accreditation of C3PAOs without the review and approval of the OUSD(A&S)/OCISO(A&S) CMMC Office.
9. In coordination with and after approval from the OUSD(A&S)/OCISO(A&S) CMMC Office, publish the current DoD and ISO/IEC accreditation requirements for C3PAOs in a downloadable document on the publicly-accessible CMMC “Marketplace” website.
10. Provide the DoD with information about the authorization and accreditation status of C3PAOs. Specifically, in response to reasonable requests for information pertaining to issues and to aggregate statistics, provide all responsive information; and in response to requests for other information regarding the status of C3PAO authorization and accreditation status, provide responsive information as mutually agreed to by the parties.
11. Provide inputs for supplemental guidance for assessors to the OUSD(A&S)/OCISO(A&S) CMMC Office. Participate and support coordination of these and other inputs through DoD-led Working Groups for consideration for inclusion into the CMMC Assessment Guides.

B. Authorization and Accreditation of CAICO

1. Authorize the CAICO to certify CMMC assessors and instructors, during the 24-month provisional period starting 31 October 2020 and ending 30 October 2022, only after verifying they have met all specified DoD requirements (to be provided to the CMMC-AB NLT 31 January 2021 via a bilateral modification and incorporation in the contract IAW

Article III.B of the terms and conditions) with the exception of achieving the ISO/IEC 17024 accreditation requirements.

2. Accredit the CAICO in accordance with ISO/IEC 17024 and specified DoD requirements.
   a. Require the CAICO to achieve and maintain the ISO/IEC 17024 accreditation requirements within 25 months of registration.
3. Establish, maintain, and manage an up-to-date list of the authorized and accredited CAICO on a publicly-accessible CMMC "Marketplace" website whose specific name and detailed function will be mutually agreed upon by the parties. The CMMC-AB shall provide a listing of this entity and its status to the DoD.
4. The CMMC-AB will provide an up-to-date list of registered candidate assessors, training records, authorized assessors, and certified assessors, registered candidate instructors, authorized instructors, and certified instructors. This data will include the dates associated with assessor or instructor training and the dates certification awards. The data will also include instructor affiliation with Licensed Training Providers and the modules they are certified to instruct. This information will be stored by the DoD in the CMMC eMASS or an alternative DoD system using the format specified by the DoD.
5. The CMMC-AB will not publish nor change requirements for the authorization and accreditation of the CAICO without review and approval by the OUSD(A&S)/OCISO(A&S) CMMC Office prior to implementation to ensure compliance with the CMMC Model, CMMC Assessment Guides and DoD policies.
6. In coordination with OUSD(A&S)/OCISO(A&S) CMMC Office, publish the current DoD accreditation requirements for the CAICO on the publicly-accessible CMMC "Marketplace" website.
7. Provide the DoD with information about the authorization and accreditation status of CACIO. Specifically, in response to reasonable requests for information pertaining to issues and to aggregate statistics, provide all responsive information; and in response to requests for other information regarding the status of CACIO authorization and accreditation status, provide responsive information as mutually agreed to by the parties.

C. Information Technology (IT) and Infrastructure

1. The CMMC-AB, C3PAOs, and the CAICO will not be allowed to store, process, handle, or transmit CUI on internal systems until those internal IT systems and/or networks meet CMMC Level 3 and are certified by DoD assessors from the Defense Contracting Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).
2. The CMMC-AB shall not store, process, handle, or transmit CUI on any external non-DoD system until such external information system is certified by Government assessors from the DCMA to be CMMC Level 3 compliant.

   - If the CMMC-AB uses an external cloud service provider to store, process, or transmit CUI, the CMMC-AB shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.
   - If the CMMC-AB uses an external cloud service provider, the CMMC-AB is responsible for addressing cybersecurity gaps that exist between the FedRAMP Moderate baseline and CMMC Level 3.
   - If the CMMC-AB selects services from an external cloud service provider that has not been FedRAMP authorized, the CMMC-AB shall hire a Third Party Assessment

Organization (3PAO) approved by the GSA FedRAMP Program Management Office to independently assess the external cloud service provider using the same assessment methodology and criteria established by GSA FedRAMP Program Management Office for a FedRAMP Moderate Baseline approval. The CMMC-AB will provide this assessment result to the DIBCAC in support of the CMMC Level 3 assessment.

3. Require all C3PAO information systems (internal and external), including any assessment tools, that store, process, or transmit CUI, to be certified CMMC Level 3 by DCMA DIBCAC assessors before conducting assessments and receiving authorization or accreditation from the CMMC-AB.
    - If a C3PAO uses an external cloud service provider to store, process, or transmit CUI, the C3PAO shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.
    - If a C3PAO selects services from an external cloud service provider that has not been FedRAMP authorized, the C3PAO shall hire a Third Party Assessment Organization (3PAO) approved by the GSA FedRAMP Program Management Office to independently assess the external cloud service provider using the same assessment methodology and criteria established by GSA FedRAMP Program Management Office for a FedRAMP Moderate Baseline approval. The C3PAO will provide this assessment result to the DIBCAC in support of the CMMC Level 3 assessment.
4. Require all independent individual assessors, who are not employees of C3PAOs, to use IT, cloud, and cybersecurity services and end-point devices provided by the accredited C3PAO whom they are supporting and who has received a CMMC Level 3 or higher certificate. Individual assessors are prohibited from using their own IT (to include internal and external cloud services) and end-point devices to store, process, handle, or transmit assessment reports and any other related information,
5. Designate CMMC-AB users who require access to the CMMC eMASS using CMMC Level 3 certified IT. The DoD must approve and authenticate these designated individuals and may deny access in its sole discretion. If the Government denies access, it will provide the CMMC-AB with the reason for denial and acceptable modes of mitigation.

D. Security

1. Require individual assessors for Level 1, based in the US, and supporting the DoD, to be a U.S. person and have a favorably adjudicated Tier 1 suitability determination that results in no security clearance.
2. Require all Level 1 assessors, who are internationally based, to meet the equivalent of a favorably adjudicated Tier 1 suitability determination that results in no security clearance.
3. Require individual assessors for Level 2 or higher, based in the US, and supporting the DoD, to be U.S. Citizens and have a favorably adjudicated Tier 3 suitability determination that results in no security clearance.
4. Require all Level 2 or higher assessors, who are internationally-based, to meet the equivalent of a favorably adjudicated Tier 3 suitability determination that results in no security clearance.
5. Require all Level 1 C3PAOs' outsourced IT, managed service provider (MSP), and managed security service provider (MSSP) support organizations staff who view or handle assessment data, either electronically or physically, to be U.S. persons and undergo a suitability

determination consistent with a favorably adjudicated Tier 1 suitability determination that results in no security clearance.

6. Require all Level 2 or higher C3PAOs' outsourced IT, MSP, and MSSP support organizations staff who view or handle assessment data, either electronically or physically to be U.S. Citizens and undergo a suitability determination consistent with a favorably adjudicated Tier 3 suitability determination that results in no security clearance.
7. The CMMC-AB shall require C3PAOs to provide proof of nationality of investors of the C3PAO, the identity of individual investors of the C3PAOs, business registration information of the C3PAO, proof and validation of the source of funds of a foreign investment or foreign funds provided to the C3PAO, the ownership structure and identities of the board members and directors of the C3PAO. The CMMC-AB shall provide this information to the DoD prior to C3PAO accreditation and when requested. Risk decisions shall be made in accordance with the attached risk matrix and the CMMC-AB shall accept no entity with a risk factor greater than medium. In extenuating circumstances, a request for a waiver may be submitted with documented mitigation steps.
   The CMMC-AB shall require certified CMMC assessors, who are employed or contracted by a C3PAO, to be citizens of the country where the C3PAO is physically located and can only assess contractors based in that country. The CMMC-AB cannot enter into any agreements with international entities without the approval of DoD.

E. Administrative

1. The OUSD(A&S)/OCISO(A) CMMC office and CMMC-AB mutually agree to protect and restrict CMMC related data or metrics for official business purposes and TO THE MAXIMUM EXTENT PRACTICABLE, ensure that data released publicly is coordinated prior to release. Both parties further agree to collaborate on CMMC program related strategic messaging to ensure alignment, and to maintain effective lines of communications between each other to facilitate program success.
2. The CMMC-AB will support DoD in establishing reciprocity and/or standard acceptance agreements with other entities for other cybersecurity standards (e.g. ISO 27001, GSA FedRAMP, DoD Standard Assessment Methodology, etc.) and shall implement processes and policies and include appropriate instruction for CMMC instructors and Certified CMMC assessors to credibly address and support such reciprocity and/or standard acceptance agreements.
3. The CMMC-AB shall establish and maintain appropriate and consistent communication channels with the Government regarding all CMMC-AB activities and shall support DoD-led Working Groups.
4. The CMMC-AB shall provide consistent and accurate monthly, quarterly and annual status update reports to the OUSD(A&S)/OCISO(A&S) CMMC Office, to include significant findings and C3PAO accreditation status, assessor certification status, and assessor training status.
5. The CMMC-AB shall participate in an annual review held by the OUSD(A&S)/OCISO(A&S) CMMC Office to determine adherence to the CMMC-AB's responsibilities as defined in this contract.
6. The CMMC-AB will not publish nor change requirements for CMMC assessors, lead assessors, assessment team members, assessment team size and composition, trainers, and instructors without the review and approval of the OUSD(A&S)/OCISO(A&S) CMMC Office.

V. DoD Responsibilities:

OUSD(A&S)/OCISO(A&S) CMMC Office will conduct the following activities in the manner described below:

1. Retain oversight of the CMMC program to include the CMMC-AB.
2. Develop, update, maintain, and publish the CMMC Model, all CMMC Assessment Guides, and policies for the DoD implementation of CMMC framework.
3. Establish specified DoD requirements in addition to ISO/IEC 17020 for the authorization and accreditation of C3PAOs.
4. Establish specified DoD requirements in addition to ISO/IEC 17024 for the authorization and accreditation of the CAICO.
5. Establish specified DoD requirements for CMMC assessors, lead assessors, assessment team members, assessment team size and composition, trainers, and instructors.
6. Establish and maintain regular coordination with CMMC-AB to include weekly telecons to coordinate on current status, and a monthly meeting to exchange status updates and discuss plans to address mid-term to far-term issues or opportunities.
7. Provide a written and recordable Summary of Conclusions of key CMMC-AB meetings and coordinate approved and dated Summary of Conclusions with CMMC AB for concurrence within three 3 business days of meeting.
8. Coordinate and synchronize all CMMC model version releases with the CMMC-AB and the DIB SCC, to provide sufficient time for CMMC-AB to inform C3PAOs and the CAICO.
9. Coordinate and synchronize all CMMC Assessment Guides version releases with the CMMC-AB and the DIB SCC to provide sufficient time for CMMC-AB to inform the C3PAOs and the CAICO.
10. Provide the CMMC-AB with initial draft training material on CMMC background information, the CMMC Model, and CMMC Assessment Guides for use by the CMMC-AB as Government Furnished Information (GFI).
11. Establish and maintain the CMMC eMASS infrastructure and provide access to the CMMC-AB as GFI. Both parties agree to identify specific responsibilities, tasks, and Service Level Agreements requirements upon contract award.
12. Grant access to CMMC eMASS to select members of C3PAOs as GFI conditioned upon users meeting DoD requirements and procuring appropriate certificates.
13. Develop the data fields requirements and templates associated with the Assessment Reports for all C3PAOs and assessors.
14. Populate and keep current a list of DIB entities and their CMMC certification level in the CMMC eMASS and Supplier Performance Risk System.
15. Communicate the requirement to achieve CMMC certification to companies in the DIB.
16. Establish reciprocity and/or standard acceptance agreements with other entities for other cybersecurity standards (e.g. ISO 27001, GSA, FedRAMP, DoD Standard Assessment Methodology, etc.). Collaborate with and seek input from the CMMC-AB and the DIB SCC in the process of establishing reciprocity and/or standard acceptance agreements.
17. Provide factual information to the CMMC-AB 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).
18. Identify programs to assist small businesses with the preparation for achieving CMMC requirements and successfully completing CMMC assessments.
19. Establish and maintain open communication channels with the CMMC-AB to include CMMC-AB participation in DoD-led Working Groups where appropriate.

20. Conduct a quarterly review with the CMMC-AB Board of Directors to assess the parties' alignment with the understandings set forth in this contract and review the annual report from the CMMC-AB.
21. Sponsor and fund Tier 3 suitability determinations for the CMMC-AB staff.
22. Sponsor and fund Tier 3 suitability determinations that result in no security clearance for C3PAO assessors conducting CMMC Level 2 -5 assessments.
23. Sponsor and fund Tier 3 suitability determinations that result in no security clearance for outsourced support IT, MSP, and MSSP staff for CMMC-AB and C3PAOs conducting Level 2-5 assessments.
24. Sponsor and fund Tier 1 suitability determinations that result in no security clearance for CMMC assessors conducting CMMC Level 1 assessments.
25. Sponsor and fund Tier 1 suitability determinations that result in no security clearance for outsourced support IT, MSP, and MSSP staff for C3PAOs conducting Level 1 assessments.
26. The DoD shall ensure that an alternative DoD system is available for temporary use in the even that CMMC eMASS is not operationally available prior to the conduct of CMMC assessments by authorized C3PAOs. To the maximum extent possible and practical, the DoD will respond to CMMC-AB requests within 2 weeks.

DCMA DIBCAC assessors will conduct the following activities in the manner described below:

1. Complete training and obtain certification from the CAICO.
2. Complete CMMC training during the provisional 24-month period prior to conducting CMMC assessments.
3. Conduct CMMC Level 3 assessments of the CMMC-AB information systems that process, store, and/or transmit CUI. DCMA DIBCAC may request augmentation from other DoD assessors on an-as needed basis.
4. Conduct CMMC assessments for candidate C3PAOs. DCMA DIBCAC may request augmentation from other DoD assessors on an-as needed basis.

VI. Performance Objectives:

Required Performance	Performance Standard	Maximum Allowable Degree of Deviation Requirement	Method of Surveillance
Provide a Comprehensive Plan / Roadmap for achieving compliance with ISO/IEC 17011 standards within no more than 2 years. As part of this plan, include a detailed risk mitigation plan for any and all identified potential conflicts of interest that may pose a risk to compliance with ISO/IEC 17011. This plan	- Completed self-assessment against the ISO/IEC 17011 standard in 1QFY21 - Identify executable steps and realistic timelines to eliminate potential conflicts of interest between (i) accreditation and DIB CMMC certification activities; and (ii) accreditation and	1 month	OUSD(A&S)/OCISO(A&S) CMMC Office review and approval of the Transition Plan / Roadmap.

must specify the establishment of the CAICO which is separate and independent from the CMMC-AB and will meet all ISO/IEC 17024 requirements.	assessor and instructor certification. 2QFY21.		
Become an approved associate member of the InterAmerican Accreditation Cooperation (IAAC) and remain in good standing.	October 31, 2021	1 month	OUSD(A&S)/OCISO(A&S) CMMC Office review of Membership status during monthly CMMC-AB reviews.
Achieve conformity with ISO/IEC 17011 to support performing accreditation body functions for ISO/IEC 17020 and ISO/IEC 17024	October 31, 2022 (or 24 months after contract signature)	1 month	Independent Peer Evaluation that verifies full compliance of all ISO/IEC 17011 requirements through peer review(s) by representatives from ISO / IEC 17011 Accreditation Bodies IAW ISO/CASCO
Conduct management reviews IAW ISO/IEC 17011 para 9.8 and provide results to the DoD CMMC program office. The annual review must include the results of the latest self-assessment and any independent, peer reviews not previously provided to the OUSD(A&S)/OCISO(A&S) CMMC Office.	Annual (to be scheduled by mutual agreement)	N/A	OUSD(A&S)/OCISO(A&S) CMMC Office annual review of CMMC-AB
Become an approved full member of InterAmerican Accreditation Cooperation (IAAC) after achieving ISO/IEC 17011 compliance and shall remain in good standing.	October 31, 2023 (or 36 months after contract signature)	1 month	OUSD(A&S)/OCISO(A&S) CMMC Office review of Membership status during monthly reviews.

VII. Deliverables:

Both parties agree that there are variables that may impact the threshold and objective delivery dates established below, and agree to reassess for reasonable consideration and relief as circumstances dictate. To be delivered to the COR for the OUSD(A&S)/ OCISO(A&S) CMMC Office:

1. ISO/IEC 17011 Compliance Roadmap and Plan that identify key planned milestones to include, but not limited to, membership in IAAC, transitioning training to an independent certification body, development of a revised business plan, dates for conducting self-assessment, peer reviews and achieving compliance. Distribution: Please submit to the COR, PMO, and KO via email.
   Threshold 2nd Quarter FY2021 Objective 1st Quarter FY2021
2. Updates and progress on ISO/IEC 17011 Compliance Roadmap and Plan to on a monthly basis. Distribution: Please submit to the COR, PMO, and KO via email.
3. Results of all ISO/IEC 17011 self-assessments, independent assessments, and peer reviews. Distribution: Please submit to the COR, PMO, and KO via email.
4. List of all current and planned subcontracts, on a monthly basis, that support the CMMC-AB in their functions as an accreditation body as well as those subcontracts that support training, assessment and consulting related activities. Distribution: Please submit to the COR, PMO, and KO via email.
5. Comprehensive Conflict of Interest (COI) and Ethics Plan: inclusive of CMMC-AB, C3PAOs, individual assessors, trainers, and others for DoD review and comment. This includes policy that prohibits any individual and C3PAO from providing paid consulting services and assessments to the same DIB contractor. This also includes policy that prohibits any CMMC-AB member or the CMMC-AB from having a conflict of interest in the execution of its responsibilities. Any proposed changes must be coordinated with the USD(A&S)/OCISO(A&S) CMMC Office prior to implementation. Distribution: Please submit to the COR, PMO, and KO via email.

   Threshold 1st Quarter FY2021
6. Communications Plan: NLT January 31 2021, Provide OUSD(A&S)/ OCISO(A&S) CMMC Office with a strategic CMMC-AB communications strategy that sets forth the CMMC-AB's approach for updating the CMMC-AB and CMMC "Marketplace" website(s) and provide updated plan when the plan is changed and notify the OUSD(A&S)/OCISO(A&S) CMMC Office of the changes during the weekly sync. Distribution: Please submit to the COR, PMO, and KO via email.
7. Quality Control Plan: inclusive of key CMMC-AB duties to include but not limited to the authorization and accreditation of C3PAOs and the CAICO, as well as the interim duties associated with training (i.e. training material development, instruction, examination, etc.).
8. Threshold 1st Quarter FY2021Change Control Procedures: The established procedures used by the CMMC-AB to process Government specified changes prior to implementation in training and testing content. The procedures shall include the CMMC-AB providing the results of the change control review, to include but not limited to, the impact, schedule, and risk analysis within 2 weeks of a Government's change request submission to the CMMC-AB. Distribution: Please submit to the COR, PMO, and KO via email.

   Threshold 1st Quarter FY2021
9. Training – Training of candidate assessors for CMMC up to Level 3 shall start:

Threshold 2nd Quarter FY2021

10. Training – Training of candidate assessors for CMMC Levels 4 & 5 shall start:

    Threshold 4th Quarter FY2021

    Objective 3rd Quarter FY2021

    - Contingent on when DoD provides the appropriate assessment guide training materials

11. Training Targets – Year 1: 360 assessors trained for up to CMMC Level 3:

    Threshold 4rd Quarter FY2021

    Objective 3rd Quarter FY2021

12. Training Targets – Year 2: 1500 assessors trained:

    Threshold 2nd Quarter FY2022

    Objective 1st Quarter FY2022 with consistent progress throughout the remainder of the contract.

13. Training Targets – Year 1: 15 assessors trained for CMMC Level 4 & 5

    Threshold 4th Quarter FY2021

    Objective 3rd Quarter FY2021

14. Training curricula (training material, videos, documents, lesson plans, and instructor notes) and examinations, test bank questions and answers. Distribution: Please submit to the COR, PMO, and KO via Safe.

    Threshold: Finalized products prior to implementation

15. Monthly status reports must be delivered the 10th day of every month to include:

    - Name of all registered, authorized and accredited C3PAOs
    - Name and affiliation of all registered, trained, and certified assessors by level
    - Status of Quality Assurance assessments conducted on C3PAOs and certified assessors
    - Number of assessors who failed training, by level and identifying the failure areas
    - Status of the authorization and accreditation of the CAICO
    - Name and affiliation of all registered and trained instructors
    - Training statistics to include number of assessors trained per training organization, average exam score and failure rates per training class by organization and instructor(s).

16. Quarterly status report documenting the metrics provided in deliverable Number 14 for each quarter of a fiscal year. Delivery Time: 30 days after each quarter. Distribution: Please submit to the COR, PMO, and KO via Safe.
17. Annual status report documenting the metrics provided in deliverable Number 14 for the fiscal year. Delivery Time: October 31, every year. Distribution: Please submit to the COR, PMO, and KO via Safe.
18. Transition out plan – Upon request, provide a transition out plan within 30 calendar days, for transfer of operations to another body in the event this contract is terminated. Distribution: Please submit to the COR, PMO, and KO via Safe.

Deliverables 1-8 must be provided to the COR, PMO, and KO via email. Deliverables 14-18 must be provided through DoD's Secure Access File Exchange (SAFE) at https://safe.apps.mil/.

TERMS AND CONDITIONS

Cybersecurity Maturity Model Certification (CMMC) Accreditation Body (AB)

Terms and Conditions

TABLE OF CONTENTS

ARTICLE I: SCOPE OF THE CONTRACT

ARTICLE II: TERM OF THE CONTRACT AND TERMINATION

ARTICLE III: CONTRACT ADMINISTRATION

ARTICLE IV: DISPUTES

ARTICLE V: CONFIDENTIAL INFORMATION

ARTICLE VI: PUBLICATION AND ACADEMIC RIGHTS

ARTICLE VII: INTELLECTUAL PROPERTY RIGHTS

ARTICLE VIII: ASSIGNMENT AND TRANSFER

ARTICLE IX: EXPORT CONTROL

ARTICLE X: OPERATIONAL SECURITY

ARTICLE XI: GOVERNING LAW AND JURISDICTION

ARTICLE XII: GOVERNMENT FURNISHED INFORMATION

ARTICL XIII: EXCLUSIVE LICENSE OR CONTRACT ARRANGEMENTS

ARTICLE XIV: SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

ARTICLE XV: STATUTORY AUTHORITY

ARTICLE XVI: INDEMNITY

ARTICLE XVII: FORCE MAJEURE

ATTACHMENTS

ATTACHMENT 1: STATEMENT OF WORK

ATTACHMENT 2: CONTRACT ADMINISTRATION

ATTACHEMNT 3: OPERATIONAL SECURITY

ARTICLE I: SCOPE OF THE CONTRACT

A. This Non-FAR or DFARS based Contract is pursuant to Fiscal Year 2020 NDAA §1648

B. Scope

1. Cyber Security Maturity Model Certification Accreditation Body, Inc. (CMMC-AB) shall be responsible for performance of the work set forth in the proposed Statement of Work (SOW), as agreed upon by the parties. The CMMC-AB shall provide all documentation required in accordance with the deliverables table set forth in the SOW.

ARTICLE II: TERM OF CONTRACT AND TERMINATION

A. Term of this Contract

The term of this Contract commences upon the date of the last signature herein and continues as defined in the contract. Provisions of this Contract, which, by their express terms or by necessary implication, apply for periods of time other than specified herein, shall be given effect, notwithstanding this Article.

B. Termination

The Government may terminate this contract, or any part hereof, for cause in the event of any default by CMMC-AB, or if CMMC-AB fails to comply, in material respects, with any contract terms and conditions, or fails to provide the Government, upon request, with adequate assurances of future performance. In addition, if the contractor fails to meet any of the Performance Objectives (inclusive of the Maximum Allowable Degree of Deviation) in the SOW Section VI, the Government may terminate this contract for cause. In the event of termination for cause, the Government shall not be liable to CMMC-AB for any amount.

The Government may terminate this Contract for convenience by written notice to the CMMC-AB, provided that such written notice is preceded by consultation between the Partiess.

C. Extending the Term

The Parties may extend, by mutual written modification, the term of this Contract if opportunities within the scope set forth in Article I reasonably warrant. Any extension shall be formalized through modification of the Contract by the Contracting Officer (KO) and the CMMC-AB and in accordance with procedures outlined in Article III, paragraph B.

D. Special Termination Clause

In the event the Government is made aware of an "outside investor" in violation of the Committee on Foreign Investment in the United States (CFIUS) or The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), this Contract will be subject to immediate termination without notification pursuant to paragraph B of this article. The CMMC-AB is encouraged to disclose outside investor activity in order for the Government to perform risk assessment of critical technology and national defense.

ARTICLE III: CONTRACT ADMINISTRATION

A. Administration

Unless otherwise provided in this Contract, approvals permitted or required to be made by the Washington Headquarters Services/Acquisition Directorate (WHS/AD) Contracting Activity may be made only by the

Contracting Officer. Administrative and contractual matters under this Contract shall be referred to the representatives identified in Attachment 2.

B. Modifications/Change of Circumstances

Each party will promptly notify the other party of any legal impediment, change of circumstances, pending litigation, or any other event or condition that may adversely affect such party's ability to carry out any of its obligations under this No-Cost Contract.

The only method by which this No-Cost Contract can be modified is through formal, written modification, signed by the KO.

1. Recommendations for modifications, including justifications to support any changes to the SOW, requirements and/or terms and conditions or any attachments thereto shall originate with either a request from the CMMC-AB to the COR and KO, or the Government through the KO. This documentation will detail the technical, chronological, and financial impact of the proposed modification to the program and requirements.

2. The KO is responsible for the review and verification of any recommendations to modify the SOW, or other proposed changes to the terms and conditions of this Contract. If additional terms and conditions are required to be included to address work that may be required under this Contract, they will be included by mutual written modification to this Contract.

3. For administrative Contract modifications (e.g. changes to Government or the CMMC-AB's personnel identified in the Contract, etc.) no signature is required by the CMMC-AB. Administrative modifications may be unilaterally executed by the KO. All modifications except for administrative modifications shall be made by mutual written Contract of the parties.

4. The KO is responsible for instituting all modifications to this Contract.

ARTICLE IV: DISPUTES

A. General

The Parties shall communicate with one another in good faith and in a timely and cooperative manner when raising issues pertaining to this Contract under this article, with the objective of resolving any misunderstanding, disagreements, claims, or disputes by mutual Contract.

B. Dispute Resolution Procedures

1. Any disagreement, claim or dispute between the Government and the CMMC-AB concerning questions of fact or law arising from or in connection with this Contract, and, whether or not involving an alleged breach of this Contract, may be raised only under this Article.

2. Whenever disputes, disagreements, or misunderstandings arise, the Parties shall attempt to resolve the issue(s) involved by discussion and mutual Contract as soon as practicable, with the goal of settlement within three (3) months of identification of the issue. Every reasonable attempt will be made to resolve all issues at the KO's level. Alternative Dispute Resolution (ADR) procedures to include, but not limited to settlement negotiations, mediation and fact-finding, will be used to the maximum extent practicable. Whenever the CMMC-AB submits, in writing, an issue to the Government, the KO shall consider the issue and, within 30 calendar days of receipt of the issue in dispute, either:

a. Prepare and transmit a written decision to the CMMC-AB, which shall include the basis for the decision, and accordingly document the Contract file or;

b. Notify the CMMC-AB of a specific date when the KO will render a decision if more time is needed for response. The notice will inform the CMMC-AB of the reason for delaying the decision.

3. In the event the CMMC-AB decides to appeal the decision, the KO shall make every effort to encourage the CMMC-AB to enter into ADR procedures with the KO. The ADR procedure applicable to this Contract expressed in subparagraphs below:

a. Failing resolution by mutual agreement, the aggrieved Party shall document the dispute, disagreement, or misunderstanding by notifying the other Party through the cognizant KO in writing documenting the relevant facts, identifying unresolved issues, specifying the clarification or remedy sought, and documenting the rationale as to why the clarification/remedy is appropriate. Within ten (10) working days after providing notice to the other Party, the aggrieved Party may, in writing, request a decision by the WHS/AD Deputy Director or designee. The other Party shall submit a written position on the matter(s) in dispute within thirty (30) calendar days after being notified that a decision has been requested. The WHS/AD Deputy Director or designee, will conduct a review of the matter(s) in dispute and render a decision in writing within thirty (30) calendar days of receipt of such position. Any such decision is final and binding, unless a Party shall, within thirty (30) calendar days request further review as provided by this article. If requested within thirty (30) calendar days of the decision by the WHS/AD Deputy Director or designee, further review will be conducted by the responsible CMMC-AB official and the WHS/AD Director or designee. In the event of a decision, or in absence of a decision within sixty (60) calendar days of referral to the responsible CMMC-AB official and the WHS/AD Director or designee (or such other period as agreed to by the parties), either party may pursue any right or remedy provided by law. Alternatively, the parties may agree to explore and establish an Alternate Disputes Resolution procedure to resolve this dispute.

b. If the CMMC-AB chooses not to participate in the Dispute Resolution Procedure or does not accept the results of the Dispute Resolution Procedure, the CMMC-AB may bring a formal claim as authorized by 28 U.S.C. § 1491 or other applicable statutes, and pursue any right and remedy in a court of competent jurisdiction. The Parties' attempt to resolve issues through settlement negotiations, mediation and fact-finding pursuant to Article IV shall be non-binding and without prejudice to either Party.

C. Limitation of Damages

Claims for damages of any nature whatsoever pursued under this Contract shall be limited to direct damages. In no event shall the Government be liable for claims for consequential, punitive, special and incidental damages, claims for lost profits, or other indirect damages.

ARTICLE V: CONFIDENTIAL INFORMATION

A. Definitions

1. “Disclosing Party” means CMMC-AB, or their subcontractors or suppliers, or the Government who discloses Confidential Information as contemplated by the subsequent Paragraphs.

2. “Receiving Party” means CMMC-AB, or their subcontractors or suppliers, or the Government who receives Confidential Information disclosed by a Disclosing Party.

3. “Confidential Information” means information and materials of or in the possession of a Disclosing Party which are designated as Controlled Unclassified Information, Confidential, or as a Trade Secret in writing by such Disclosing Party, whether by letter or by use of an appropriate stamp or legend, prior to or at the same time any such information or materials are disclosed by such Disclosing Party to the Receiving Party. Notwithstanding the foregoing, materials and other information which are orally, visually, or electronically disclosed by a Disclosing Party, or are disclosed in writing without an appropriate letter, stamp, or legend, shall constitute Confidential Information or a Trade Secret if such Disclosing Party, within thirty calendar days after such disclosure, delivers to the Receiving Party a written document or documents describing the material or information and indicating that it is confidential or a Trade Secret, provided that any disclosure of information by the Receiving Party prior to receipt of such notice shall not constitute a breach by the Receiving Party of its obligations under this Paragraph. “Confidential Information” includes any information and materials considered a Trade Secret by the CMMC-AB on its own behalf or on behalf of their subcontractors or suppliers, and any information and materials considered to be Controlled Unclassified Information by the Government on its own behalf or on behalf of its contractors or other third parties.

4. “Trade Secret” means all forms and types of financial, business, scientific, technical, economic, or engineering or otherwise proprietary information, including, but not limited to, patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes,

procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if:

a. The owner thereof has taken reasonable measures to keep such information secret; and

b. The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public.

B. Exchange of Information

The Government may from time to time disclose Confidential Information to the CMMC-AB and its subcontractors or suppliers and the CMMC-AB and its subcontractors or suppliers, may from time to time disclose information that is Trade Secret or Confidential Information to the Government in connection with the contract or performance thereunder. Neither the Government nor CMMC-AB or their subcontractors or suppliers shall be obligated to transfer Confidential Information or Trade Secrets in the possession of or independently developed by the Government or the CMMC-AB or their subcontractors or suppliers, except as required by the terms of this Contract or another express written Contract between the Parties providing the terms and conditions for such disclosure.

C. Confidentiality and Authorized Disclosure.

The Receiving Party agrees, to the extent permitted by law, that Confidential Information and Trade Secrets shall remain the property of the Disclosing Party (no one shall disclose unless they have the right to do so), and that, unless specified in this Contract or otherwise agreed to by the Disclosing Party, Confidential Information and Trade Secrets may be used by the Parties only in performance of this Contract and shall not be disclosed, divulged, or otherwise communicated by it to third parties or used by it for any other purposes, except that the Parties may disclose the information to their attorneys and, provided that the duty to protect such “Confidential Information” and “Trade Secrets” shall not extend to materials or information that:

1. Are received or become available without restriction to the Receiving Party under a proper, separate Contract,

2. Are not identified with a suitable notice or legend per Article entitled "ConfidentialInformation" herein,

3. Are lawfully in possession of the Receiving Party without such restriction to the Receiving Party at the time of disclosure thereof as demonstrated by prior written records,

4. Are or later become part of the public domain through no fault of the Receiving Party,

5. Are received by the Receiving Party from a third party having no obligation of confidentiality to the Disclosing Party that made the disclosure,

6. Are developed independently by the Receiving Party without use of Confidential Information or Trade Secrets as evidenced by written records,

7. Are required by law or regulation to be disclosed; provided, however, that the Receiving Party has provided written notice to the Disclosing Party promptly so as to enable such Disclosing Party to seek a protective order or otherwise prevent disclosure of such information.

In addition, nothing in this Contract restricts the Government’s rights under another Government contract to use technical data, computer software, or inventions. The exercise of those rights will not be a breach of this Contract.

D. Return of Proprietary Information

Upon termination, and absent mutual agreement to alternative procedures, the parties will control any proprietary data in accordance with Article VII, Intellectual Property.

E. Term

Except to the extent covered by and subject to other provisions of this Contract or the specific Project Contract, the obligations of the Receiving Party under this Article shall continue for a period of five (5) years after the expiration or termination of this Contract.

F. Subcontracts

The Government and the CMMC-AB shall flow down the requirements of this Article to their respective personnel, agents, partners, and team members receiving such Confidential Information or Trade Secrets under this no cost contract.

ARTICLE VI: PUBLICATION AND ACADEMIC RIGHTS

Subject to the provisions of Article V, Confidential Information, Attachment 3 Operational Security, and this Article Publication and Academic Rights, the CMMC-AB and the Government shall have the right to publish or otherwise disclose information and/or data developed by the Government and/or the CMMC-AB under this Contract. The CMMC-AB and the Government (and its employees) shall include an appropriate acknowledgement of the sponsorship by the Government and the CMMC-AB in such publication or disclosure. The Parties shall have only the right to use, disclose, and exploit any such data and Confidential Information or Trade Secrets in accordance with the rights held by them pursuant to this Contract. Notwithstanding the above, the Parties shall not be deemed authorized by this paragraph, alone, to disclose any Confidential Information or Trade Secrets of the Government or the CMMC-AB.

ARTICLE VII: Intellectual Property Rights

A. Definitions

1. “Government purpose” means any activity, contract, or agreement in which the United States Government is a party. Government purposes include competitive procurement, but do not include the rights to use, modify, reproduce, release, perform, display, or disclose data for commercial purposes or authorize others to do so.

2. “Data” means recorded information, regardless of the form or method of the recording, including scientific, technical, administrative, or management information, that is furnished to the Government by the CMMC-AB, C3PAOs, CAICOs, or CMMC assessors.

3. “Assessment and accreditation data” means data that is assessor and instructor registration information, credential records, instructor and assessor certification and training records, C3PAO registration information, authorization and accreditation records, CAICO registration information, authorization and accreditation records, pre-assessment information, assessment reports, defense industrial base company CMMC certifications, or dispute resolution results.

4. “Training Data” means data that is CMMC training curriculum, CMMC training materials, or associated CMMC exams.

5. “Government support contractor” means a contractor under a Government contract or agreement, the primary purpose of which is to furnish independent and impartial advice or technical assistance directly to the Government in support of the Government’s management and oversight of the CMMC effort (rather than to directly furnish CMMC-related services or products).

B. Data Rights

1. The CMMC-AB grants or shall obtain for the Government a royalty free, world-wide, nonexclusive, irrevocable license right to: 1) use, modify, reproduce, release, perform, display, or disclose assessment and accreditation data within the Government without restriction; and 2) release or disclose assessment and accreditation data outside the Government and authorize persons to whom release or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose assessment and accreditation data for United States government purposes.

2. The CMMC-AB grants or shall obtain for the Government a royalty free, world-wide, nonexclusive, irrevocable license right to: 1) use, modify (to support document review), reproduce, release, display, or disclose the training data within the Government for the purpose of reviewing the training data to ensure compliance with DOD standards (including DOD-specified requirements, the CMMC model, and the CMMC assessment guides); and 2) release or disclose training data to Government support contractors and authorize Government support contractors to use, modify (to support document review), reproduce,

release, display, or disclose the training data within the Government for the purpose of reviewing the training data to ensure compliance with DOD standards (including DOD-specified requirements, the CMMC model, and the CMMC assessment guides).

3. The CMMC-AB, C3PAOs, and CMMC assessors agree not to distribute the following categories of data to third parties: pre-assessment information, assessment reports, assessor notes, CMMC certifications, and dispute resolution results.

4. Whenever any data is to be furnished to the Government by a C3PAO, CAICO, or CMMC assessor under this Contract, the CMMC-AB shall require this same clause be included in contracts, subcontracts or other contractual instruments with C3PAOs and CAICOs (and in the subcontracts of C3PAOs and CAICOs), without alteration, except to identify the parties. No other clause shall be used to diminish the Government's rights in data furnished by a C3PAO, CAICO, or CMMC assessor.

C. Marking Requirements

With the exception of assessment and accreditation data that is entered directly into Government databases, the CMMC-AB, C3PAOs, and CAICOs shall conspicuously and legibly mark data furnished to the Government in accordance with the provisions below. Only the following legends, markings for Confidential Information in accordance with Article V of this Contract, and/or a notice of copyright as prescribed under 17 U.S.C. § 401 or § 402 are authorized under this contract. If data is furnished to the Government without any of the aforementioned legends (with the exception of assessment and accreditation data that is entered directly into Government databases), the Contractor agrees that such data is furnished to the Government without restrictions.

1. Assessment and accreditation data shall be marked with the following legend:

Contract Identifier: HQ003420H0003

Name of Copyright Owner:

Address of Copyright Owner:

In accordance with Article VII of the contract between the CMMC-AB and the Government, the Government is granted a royalty free, world-wide, nonexclusive, irrevocable license right to: 1) use, modify, reproduce, release, perform, display, or disclose assessment and accreditation data within the Government without restriction; and 2) release or disclose assessment and accreditation data outside the Government and authorize persons to whom release or disclosure has been made to use, modify, reproduce, release, perform, display, or disclose assessment and accreditation data for United States government purposes. Any reproduction of assessment and accreditation data or portions thereof marked with this legend must also reproduce these markings.

2. Training data shall be marked with the following legend:

Contract Identifier: HQ003420H0003

Name of Copyright Owner:

Address of Copyright Owner:

In accordance with Article VII of the contract between the CMMC-AB and the Government, the Government is granted a royalty free, world-wide, nonexclusive, irrevocable license right to: 1) use, modify (to support document review), reproduce, release, display, or disclose the training data within the Government for the purpose of reviewing the training data to ensure compliance with DOD standards (including DOD-specified requirements, the CMMC model, and the CMMC assessment guides); and 2) release or disclose training data to Government support contractors and authorize Government support contractors to use, modify (to support document review), reproduce, release, display, or disclose the training data within the Government for the purpose of reviewing the training data to ensure compliance with DOD standards (including DOD-specified requirements, the CMMC model, and the CMMC assessment guides).

D. Trademarks and Disclaimers

The Parties agree that the Government is the owner of all trademark rights, statutory, common law or otherwise, and the associated goodwill, in and to any trademark, service mark, or trade dress, including,

but not limited to, any word, name, phrase, symbol, design, logo, slogan, tagline, or device, or any combination thereof (hereinafter "CMMC-related marks") that is/was first proposed, suggested, described, or used by the Government, in connection with any CMMC-related products or services, or a description thereof, under this Contract. No license, implied or otherwise, to use such CMMC-related marks in connection with any goods or services anywhere in the world, is hereby granted to the CMMC-AB, C3PAOs, CAICOs, CMMC assessors, or any third party, without a prior written authorization of the Government.

The CMMC-AB shall provide the following disclaimer on all training materials, letterhead, or any publicly released materials or documents.

"CMMC-AB is a private corporation that accredits candidate C3PAOs and the CAICO under a contract with the Department of Defense."

The quoted language directly above may be revised as the CMMC-AB's 501(c)(3) status changes.

E. No Implied Licenses

Nothing in this Contract shall be construed as conferring by implication, estoppel or otherwise any license or right under any patent, copyright, trade secret, trademark or other proprietary right of either Party, except as specifically set forth herein.

F. Term

The obligations of the Parties under this Article shall survive in perpetuity after the expiration or termination of this Contract.

Article VIII: EXCLUSIVE LICENSE OR CONTRACT ARRANGEMENTS

The CMMC AB agrees that it will not establish any exclusive license or contract arrangement with any entity whose purpose is to develop or conduct CMMC training; develop and administer CMMC examinations; or certify CMMC instructors and assessors; or manage and conduct CMMC assessments.

ARTICLE IX. Assignment and Transfer

Neither Party may assign, reassign, or transfer such Party's rights and obligations under this Contract without the prior written consent of the other Party.

ARTICLE X: Export Control

A. Export Compliance

Each Party agrees to comply with U.S. Export regulations including, but not limited to, the requirements of 22 U.S.C. § § 2751-2794, including 22 C.F.R. § 120 et seq.; and the Export Administration Act. Each party is responsible for obtaining from the Government export licenses or other authorizations/approvals, if required, for information or materials provided from one party to another under this Contract. Accordingly, the CMMC-AB shall not export, directly, or indirectly, any products and/or technology, Confidential Information, Trade Secrets, or Classified and Unclassified Technical Data in violation of any U.S. Export laws or regulations.

B. Lower Tier Contracts

The CMMC-AB shall include this Article, suitably modified, to identify the Parties, in all subcontracts or lower tier Contracts, regardless of tier, for experimental, developmental, or research work.

ARTICLE XI: OPERATIONAL SECURITY

Access and General Protection/Security Policy and Procedures. All CMMC-AB employees, including subcontractor employees, shall comply with all installation and facility access and local security policies and procedures (provided by Government representative), and security/emergency management exercises. The CMMC-AB shall also provide all information required for background checks to meet installation access requirements to be accomplished by the Installation Provost Marshal Office, Director of Emergency Services, or Security Office. The CMMC-AB workforce shall comply with all personal identity verification and accountability requirements as directed by DoD, and/or local

policy. Should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in CMMC-AB security matters or processes. During FPCONs Charlie and Delta, services/installation access may be discontinued/postponed due to higher threat. CMMC-AB personnel working on an installation shall participate in the installation Random Antiterrorism Measures Program as directed. The CMMC-AB shall be subject to and comply with vehicle searches, wearing of ID badges, etc. The CMMC-AB shall comply with all requirements contained in ATTACHMENT 3 of this Contract.

ARTICLE XII: GOVERNING LAW AND JURISDICTION

This Contract shall be construed and enforced in accordance with the laws of the United States in a Federal Court with competent jurisdiction. Any dispute arising under this Contract shall first be handled in accordance with Article IV: Disputes of this Contract.

In the event that any provisions contained in this Contract or any part thereof shall for any reason be held invalid, illegal or unenforceable in any respect by a court of competent jurisdiction, to such extent such provision shall be deemed null and void and severed from this Contract, and the remainder of this Contract shall remain in full force and effect. The headings appearing at the beginning of the sections contained in this Contract have been inserted for identification and reference purposes only and shall not be used in the construction and interpretation of this Contract.

ARTICLE XIII: GOVERNMENT FURNISHED INFORMATION

The Government will provide the CMMC-AB with the Government Furnished Information (GFI) as listed in the SOW to facilitate the performance of this no cost contract.

The CMMC-AB shall assume the risk of and be responsible for any loss or destruction of, or damage to, the GFI while it is in the CMMC-AB's possession or control. The GFI shall be returned or destroyed at the end of the contract Period of Performance in accordance with the terms of the no cost contract regarding its use. The CMMC-AB shall obtain explicit written authorization for any transfer or disposition of the GFI.

ARTICLE XIV: SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

A. Definitions

1. "Adequate security" means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

2. "Compromise" means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

3. "CMMC-AB attributional/proprietary information" means information that identifies the CMMC-AB, whether directly or indirectly, by the grouping of information that can be traced back to the CMMC-AB (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the CMMC-AB.

4. "Controlled technical information" means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

5. "Covered CMMC-AB information system" means an unclassified information system that is owned, or operated by or for, a CMMC-AB and that processes, stores, or transmits covered defense information.

6. "Covered defense information" means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at

http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies, and is—

a. Marked or otherwise identified in the contract, task order, or delivery order and provided to the CMMC-AB by or on behalf of DoD in support of the performance of the contract; or

b. Collected, developed, received, transmitted, used, or stored by or on behalf of the CMMC-AB in support of the performance of the contract.

7. “Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

8. “Forensic analysis” means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

9. “Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

10. “Malicious software” means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

11. “Media” means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered CMMC-AB information system.

12. “Operationally critical support’’ means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

13. “Rapidly report” means within 72 hours of discovery of any cyber incident.

14. “Technical information” means technical data or computer software. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

B. Adequate Security

The CMMC-AB shall provide adequate security on all covered CMMC-AB information systems. To provide adequate security, the CMMC-AB shall implement, at a minimum, the following information security protections:

1. For covered CMMC-AB information systems that are part of an Information Technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

a. Cloud computing services shall be subject to the security requirements specified:

i. The CMMC-AB shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with the Cloud Computing Security Requirements Guide (SRG) found at http://iase.disa.mil/cloud_security/Pages/index.aspx, unless notified by the Contracting Officer Representative that this requirement has been waived by the DoD Chief Information Officer.

ii. The CMMC-AB shall maintain within the United States or outlying areas all Government data that is not physically located on Government premises, unless the CMMC-AB receives written notification from the Contracting Officer Representative to use another location.

iii. Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

2. For covered CMMC-AB information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph B.1. of this clause, the following security requirements apply:

a. The covered CMMC-AB information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at https://csrc.nist.gov/publications/sp800) in effect at the time the contract is issued or as authorized by the KO.

b. The National Institute of Standards and Technology Considerations:

(1) The CMMC-AB shall implement NIST SP 800-171 and a minimum of CMMC Level 3, prior to handling any CUI.

(2) The CMMC-AB shall submit requests to vary from NIST SP 800-171 in writing to the KO, for consideration by the DoD CIO. The CMMC-AB need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be non-applicable or to have an alternative, but equally effective, security measures that may be implemented in its place.

(3) If the DoD CIO has previously adjudicated the CMMC-AB's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the KO or Contracts Officer Representative when requesting its recognition under this Contract.

(4) If the CMMC-AB intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the CMMC-AB shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs C through G of this article for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

3. Apply other information systems security measures when the CMMC-AB reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

C. Cyber Incident Reporting Requirement

1. When the CMMC-AB discovers an incident that affects a covered CMMC-AB information system or the covered defense information residing therein, or that affects the CMMC-AB's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the Contract, the CMMC-AB shall—

a. Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered CMMC-AB information system(s) that were part of the cyber incident, as well as other information systems on the CMMC-AB's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the CMMC-AB's ability to provide operationally critical support; and

b. Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.

2. Cyber incident report. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil.

3. Medium assurance certificate requirement. In order to report cyber incidents in accordance with this clause, the CMMC-AB or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.

D. Malicious software.

When the CMMC-AB or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) at this website: https://www.dc3.mil/ or

in accordance with additional instructions provided by DC3 or the KO or the Contracting Officer Representative. Do not send the malicious software to the KO or Contracting Officer Representative.

E. Media preservation and protection.

When a CMMC-AB discovers a cyber incident has occurred, the CMMC-AB shall preserve and protect images of all known affected information systems identified in paragraph C.1.a. of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

F. Access to additional information or equipment necessary for forensic analysis.

Upon request by DoD, the CMMC-AB shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

G. Cyber incident damage assessment activities.

If DoD elects to conduct a damage assessment, the KO will request that the CMMC-AB provide all of the damage assessment information gathered in accordance with paragraph E of this clause.

H. DoD safeguarding and use of CMMC-AB attributional/proprietary information.

The Government shall protect against the unauthorized use or release of information obtained from the CMMC-AB (or derived from information obtained from the CMMC-AB) under this clause that includes CMMC-AB attributional/proprietary information, including such information submitted in accordance with paragraph C Cyber Incident Reporting. To the maximum extent practicable, the CMMC-AB shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the CMMC-AB attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

I. Use and release of CMMC-AB attributional/proprietary information not created by or for DoD.

Information that is obtained from the CMMC-AB (or derived from information obtained from the CMMC-AB) under this clause that is not created by or for the Government is authorized to be released outside of Government-

1. To entities with missions that may be affected by such information;

2. To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

3. To Government entities that conduct counterintelligence or law enforcement investigations;

4. For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236).

J. Use and release of CMMC-AB attributional/proprietary information created by or for DoD.

Information that is obtained from the CMMC-AB (or derived from information obtained from the CMMC-AB) under this Article that is created by or for the Government (including the information submitted pursuant to paragraph C of this article) is authorized to be used and released outside of the Government for purposes and activities authorized by paragraph a. of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

K. Other safeguarding or reporting requirements.

The safeguarding and cyber incident reporting required by this clause in no way abrogates the CMMC-AB's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

L. Lower Tier Contracts

The CMMC-AB shall include this Article, suitably modified to identify the Parties, in all subcontracts or lower tier Contracts entered into solely in connection with this Contract.

ARTICLE XV: STATUTORY AUTHORITY

This Contract is not a Federal procurement contract, grant or cooperative agreement. Nothing in this Contract or its attachments will be construed as incorporating by reference or implication any provision of Federal acquisition law or regulation not specifically mentioned in this Contract. This Contract is subject to the compliance requirements of Title VI of the Civil Rights Act of 1964 as amended (42 U.S.C. § 2000d) relating to nondiscrimination in Federally assisted programs. The CMMC-AB has signed an Assurance of Compliance with the nondiscriminatory provisions of the Act. Additionally, this Contract is subject to the Trafficking Victims Protection Act of 2000, as amended (22 U.S.C. chapter 78), Executive Order 13627, Strengthening Protections Against Trafficking in Persons in Federal Contracts, the international Traffic in Arms Regulations (22 C.F.R. Part 120, et seq.), the National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M), the Department of Commerce's Export Administration Regulations (15 C.F.R. Part 730, et seq.).

ARTICLE XVI: INDEMNITY

A. The CMMC-AB shall defend, indemnify and hold the Government harmless (including payment of all reasonable costs, attorneys' fees, settlements and damages) from any actions brought against Government to the extent that it is based on a claim that any materials the CMMC-AB delivers to the Government (the "Materials") infringe any U.S. registered copyright of any third party, provided that the CMMC-AB is promptly notified in writing of the claim.

B. In the event of any such infringement claim, the CMMC-AB may at its sole option:

1. replace the infringing Products with functionally equivalent software;

2. modify such Products to render the same non-infringing, while retaining substantively equivalent functionality

3. procure for the Government a license to continue to use such Products under the terms of this Contract; or

4. if the foregoing are not commercially reasonable, direct the Government to terminate use of such Products.

C. Notwithstanding the foregoing, the CMMC-AB will have no liability with respect to any claim that arises from any such infringement claim to the extent that it results from: (i) use, operation, or combination of the Products or Documentation with programs, data, equipment, or materials not provided by the CMMC-AB if such infringement would have been avoided by the use of the Products or Documentation without such other programs, data, equipment, or materials; (ii) modifications to the Products made by a party other than CMMC-AB or its agents; (iii) data accessed or generated by the Products (including, without limitation Third Party Materials); (iv) the combination, operation or use of the Products with equipment, devices, data or software not provided or approved by CMMC-AB; (v) the Government's failure to use updated or modified versions of the Products provided by CMMC-AB to avoid a claim; (vi) CMMC-AB's compliance with any specifications or requirements provided by Government; or (vii) the Government's use of the Products other than in accordance with this Contract.

D. This article specified the Government's sole and exclusive remedy and the CMMC-AB'S sole and exclusive obligation with respect to the infringement of intellectual property rights.

E. The Government shall not indemnify any entity. The Government agrees to pay for any loss, liability or expense, which arises out of or relates to the Government's acts or omissions with respect to its obligations hereunder, where a final determination of liability on the part of the Government is established by a court of law, or where settlement has been agreed to by the Government agency with, where appropriate, the coordination of the Department of Justice. This provision shall not be construed to limit the Government's rights, claims or defenses which arise as a matter of law or pursuant to any other provision of this Contract

F. The CMMC-AB will file a streamlined request to the U.S. Department of Homeland Security for the issuance of a "Pre-Qualification Designation Notice" under the Support Anti-Terrorism by Fostering Effective Technolgies Act of 2002 ("SAFETY ACT") (6 U.S.C. § 441, 6 CRF Part 25) that will encompass the servcies offered by the AB as defined under this SOW.

ARTICLE XVII: FORCE MAJEURE

Neither Party shall be in breach of this Contract for any failure of performance caused by any event beyond its reasonable control and not caused by the fault or negligence of that Party including but not limited to, the following: acts of God; acts or omissions of any Government; any rules, regulations or orders issued by any Governmental authority or by any officer, department, and agency or instrumentality thereof; fire; epidemics, pandemics, storm; flood; earthquake; accident; war; rebellion; insurrection; riot; and invasion. If such a force majeure event occurs, the Party unable to perform shall promptly notify the other Party and shall in good faith maintain such partial performance as is reasonably possible and shall resume full performance as soon as is reasonably possible.

ATTACHMENT 1: STATEMENT OF WORK (SOW)

See attachment.

ATTACHMENT 2: CONTRACT ADMINISTRATION

Below is a list of the Points of Contact for the CMMC-AB and the Government. Each Party may change its representatives named below by written notification to the other party. The Government will affect the change following the procedures in Article II, subparagraph C.3. of the main text of the Contract.

A. Government Points of Contact:

Contracts Officer (KO):

Name: (b)(6)

Phone:

Email:

Contracts Officer Representative

Name: (b)(6)

Phone:

Email:

B. CMMC-AB's Points of Contact

Director CMMC-AB Board of Directors:

As included in the contract file.

Acting Chairman CMMC-AB Board of Directors:

As included in the contract file.

ATTACHMENT 3: OPERATIONAL SECURITY

A. Access and General Protection/Security Policy and Procedures. The CMMC-AB shall provide personnel with the appropriate personnel security clearance levels for the work to be performed. Access to classified information is required in the performance of this contract and shall be in accordance with the DoD 5220.22-M, National Industrial Security Program Operating Manual (NISPOM), applicable DoD personnel security regulations. The CMMC-AB shall maintain sufficiently cleared personnel to perform the tasks required by this SOW and the Contract. All CMMC-AB personnel shall possess the requisite security clearance, accesses, and need-to-know commensurate with the requirements of their positions. Overarching contract security requirements, and CMMC-AB access to classified information, shall be as specified in the basic DD Form 254 for this task order. All CMMC-AB personnel with access to unclassified IS, including e-mail, shall have at a minimum a favorable DoD sponsored National Agency Check with Inquiries (NACI).

B. Security Education, Training and Awareness Briefs: All CMMC-AB employees, including subcontractor employees, shall receive new employee training and annual security refreshers. These training programs will be used to inform employees of the types of behavior to watch for and instruct employees to report suspicious activity and violations to their local security officers. This training shall be completed within 45 calendar days after contract start date or effective date of incorporation of this requirement into the contract, whichever applies, and then annually thereafter. The CMMC-AB shall submit certificates of completion for each affected CMMC-AB employee and subcontractor employee to the COR within 14 calendar days after completion of training by all employees and subcontractor personnel.

C. Access to DoD Facility or Installation: All CMMC-AB employees, including subcontractor employees, shall comply with adjudication standards and procedures using the National Crime Information Center Interstate Identification Index (NCIC-III) and Terrorist Screening Database (DoDM 5200.08-R 09APR07); applicable installation, facility and area commander installation and facility access and local security policies and procedures (provided by the COR).

D. Information Technology/Information Assurance: The CMMC-AB shall be capable of accessing, handling, receiving and storing UNCLASSIFIED documents, equipment, hardware and test items using the applicable standards of For Official Use Only (FOUO) information. All Controlled Unclassified Information (documents designated as FOR OFFICIAL USE ONLY and/or LIMITED DISTRIBUTION) shall be submitted by a controlled means using UPS mail.

E. For Official Use Only Information (FOUO) and Controlled Unclassified Information (CUI): CMMC-AB personnel shall be capable of accessing, handling, receiving and storing UNCLASSIFIED documents, equipment, hardware and test items using applicable standards of FOUO and CUI. For Official Use Only information generated and/or provided under this contract shall be marked and safeguarded as specified in DoDM 5200.01, Information Security Program Manual (Volume 4) available at http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf. The CMMC-AB shall not store or transmit CUI on personal IT systems or via personal e-mail. Unclassified e-mail containing any DoD CUI shall be encrypted.

F. Operations Security (OPSEC):

1. The CMMC-AB shall develop, implement, and maintain an OPSEC program to protect controlled unclassified and classified activities, information, equipment, and material used or developed by the CMMC-AB and any subcontractor during performance of the contract. The CMMC-AB shall be responsible for the subcontractor implementation of the OPSEC requirements. The OPSEC program shall be in accordance with National Security Decision Directive (NSDD) 298, and at a minimum shall include:

a. Assignment of responsibility for OPSEC direction and implementation.
b. Issuance of procedures and planning guidance for the use of OPSEC techniques to identify vulnerabilities and apply applicable countermeasures.

c. Establishment of OPSEC education and awareness training.
d. Provisions for management, annual review, and evaluation of OPSEC programs.
e. Flow down of OPSEC requirements to subcontractors when applicable.

2. The CMMC-AB shall prepare an Operations Security Plan in accordance with DODM 5205.02 for Government review.

3. The CMMC-AB shall implement and maintain security procedures and controls to prevent unauthorized disclosure of controlled unclassified and classified information and to control distribution of controlled unclassified and classified information in accordance with the National Industrial Security Program Operating Manual (NISPOM) and DoDM 5200.01, Information Security Manual. The DoD Contract Security Classification Specification, DD Form 254, defines program specific security requirements. All CMMC-AB facilities shall provide an appropriate means of storage for controlled unclassified and classified documents, classified equipment and materials and other equipment and materials.

G. Public Release of Information: In accordance with DoDM 5205.02-M, an OPSEC review will be performed by the Government prior to all public release of information. All Government information intended for public release by a CMMC-AB shall undergo a Government OPSEC review prior to release. The OPSEC review will be performed as part of the Public Review Process described in Article VI.

The Cybersecurity Maturity Model Certification Accreditation Body

Statement of Work (SOW)

I. Purpose:

The Department of Defense (DoD) will use the Cybersecurity Maturity Model Certification – Accreditation Body, Inc. (CMMC-AB), a non-profit organization, as the authoritative source to accredit CMMC Third Party Assessment Organizations (C3PAOs) and the CMMC Assessors and Instructors Certification Organization (CAICO). The DoD will retain oversight of the CMMC program and will be responsible for establishing CMMC assessment and training requirements as well as developing, updating, maintaining, and publishing the CMMC Model, all CMMC Assessment Guides, and policies for the DoD implementation of the CMMC framework.

II. 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. OUSD(A&S) is committed to working with the Defense Industrial Base (DIB) sector to enhance the protection of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within the supply chain. 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, which is available at https://www.acq.osd.mil/cmmc/.

The CMMC Model combines various standards, references, and best practices into a unified standard. The model aligns sets of cybersecurity practices and maturity processes with the sensitivity of information to be protected and the associated threats. The CMMC framework builds upon existing regulations and efforts by adding a verification component and assessing the implementation of cybersecurity requirements.

The CMMC-AB shall accredit C3PAOs ~~and the CAICO~~ in accordance with International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) standards. The CMMC-AB will ensure that the CAICO be accredited under ISO/IEC 17024 by a recognized, U.S.-based ISO/IEC 17011 accreditation body. Through these activities, the CMMC-AB will be instrumental to the Department achieving its goal of improving the DIB sector's cybersecurity posture.

III. General Provisions:

1. This is a no cost contract. CMMC-AB shall provide all services as required by the contract at no direct cost or "gratuitously" to the Government. The Government shall not be liable for any payment arising under the contract.
2. This agreement does not impact future understandings or arrangements between the parties and does not affect the ability of the parties to enter into other understandings or arrangements with each other related to this no cost contract or any subsequent amendments.
3. The DoD grants the right to the CMMC-AB to serve as the exclusive accreditation body to support the execution of CMMC in accordance with DoD policies and requirements to include the CMMC Model and CMMC Assessment Guides.
4. The CMMC-AB shall achieve compliance with the current ISO/IEC 17011 standard no later than ~~31 October 2022~~30 April 2023. The CMMC-AB shall complete the peer assessment of

conformity in accordance with the ISO Committee on Conformity Assessment (CASCO) and demonstrate compliance with all ISO/IEC 17011 requirements no later than ~~31 October 2022~~30 April 2023.

a. The CMMC-AB, upon achieving ISO/IEC 17011 compliance, shall maintain compliance with the ISO/IEC 17011 standard to include meeting all requirements for self-assessments, peer reviews, and other assessments.

b. The CMMC-AB shall become a full member of InterAmerican Accreditation Cooperation (IAAC) after achieving ISO/IEC 17011 compliance and shall remain in good standing.

5. During the two year period starting 31 October 2020 and ending ~~30 October 2022~~April 30, 2023, the CMMC-AB shall achieve ISO/IEC 17011 compliance through the appropriate peer review process. The CMMC-AB shall:

a. Become an associate member of the InterAmerican Accreditation Cooperation (IAAC) and remain in good standing.

b. Develop and update a comprehensive plan and schedule to comply with all ISO/IEC 17011 requirements. As part of this plan, include a detailed risk mitigation plan for all potential conflicts of interest that may pose a risk to compliance with ISO/IEC 17011.

c. Develop, maintain, and provide provisional training, including curricula and testing, for instructors and individual assessors. The CMMC-AB shall coordinate all provisional training and testing content with the OUSD(A&S)/OCISO(A&S) CMMC Office for review prior to implementation to ensure compliance with the CMMC Model, CMMC Assessment Guides and DoD policies and, to verify conformance with the Government requirements specification. The Government specification is subject to change control procedures that include, but are not limited to, impact, schedule, and risk analysis. The outcome of the change control procedures will be mutually agreed upon with the Government.

d. Ensure the quality control of all training products, instruction, and testing to include reviews with respect to cybersecurity technical accuracy and alignment with the CMMC Model, CMMC Assessment Guides, and DoD cybersecurity requirements and policies.

e. Develop, maintain, and manage database(s) to track the status of all authorized and accredited C3PAOs, provisional assessors, trainers and instructors. All data shall be replicated and backed up daily to CMMC eMASS or an alternative DoD system.

f. The CMMC-AB shall provide documentation showing the CMMC-AB's current ecosystem, which includes but is not limited to C3PAOs, the CAICO, Assessors, Registered Provider Organizations, Registered Practitioners, Licensed Instructors, Licensed Partner Publisher, and Licensed Training Providers. These shall be in strict compliance with the specified DoD requirements referred to in Section III(6) below. The CMMC-AB shall provide the OUSD(A&S)/OCISO(A&S) CMMC Office with all plans and/or changes related to CMMC-AB activities and the CMMC ecosystem to review prior to implementation and publication.

6. The CMMC-AB shall develop and maintain a quality assurance program with respect to the accreditation of C3PAOs and the CAICO in accordance with ISO/IEC 17011 and specified DoD requirements to be provided to the CMMC-AB NLT 31 January 2021 via a bilateral modification and incorporation in the contract IAW Article III.B of the terms and conditions.

7. The CMMC-AB shall provide all plans that are related to potential sources of revenue to include but not limited to fees, licensing, membership, and/or partnerships to the

OUSD(A&S)/OCISO(A&S) CMMC Office. The OUSD(A&S)/OCISO(A&S) CMMC Office must acknowledge receipt and provide suggested guidance for compliance prior to the CMMC-AB implementing and publicizing.

8. The CMMC-AB Board of Directors, professional staff, Information Technology (IT) staff, accreditation staff, and contracted independent assessor staff shall be U.S. citizens shall achieve a favorably adjudicated Tier 3 suitability determination.
9. The OUSD(A&S)/OCISO(A&S) CMMC Office has the responsibility to establish the requirements for CMMC assessment and training certifications and the accreditation requirements for C3PAOs and the CAICO. OUSD(A&S)/OCISO(A&S) CMMC Office will also develop, update, maintain, and publish the CMMC Model and all CMMC Assessment Guides. The CMMC Model contains the cybersecurity requirements by which all DIB companies will be assessed against. The CMMC Assessment Guides shall serve as the singular authoritative reference for the conduct of assessments and associated activities to be used by DIB contractors, C3PAOs, assessors, training organizations and instructors, and the CMMC-AB.
10. The OUSD(A&S)/OCISO(A&S) CMMC Office shall establish and maintain the single DoD database or an alternative DoD system, to store and process assessment related data elements and the associated assessment reports. The OUSD(A&S)/OCISO(A&S) CMMC Office will provide C3PAOs and the CMMC-AB the appropriate access to perform their respective functions.

IV. CMMC-AB Duties:

A. Authorization and Accreditation of C3PAOs

1. Authorize C3PAOs to conduct CMMC assessments, during the 24-month period starting 31 October 2020 and ending 30 October 2022. Prior to authorizing any C3PAO to conduct CMCC assessments, the CMMC-AB shall verify that the C3PAO has met all specified DoD requirements (to be provided to the CMMC-AB NLT 31 January 2021 via a bilateral modification and incorporation in the contract IAW Article III.B of the terms and conditions) with the exception of achieving the ISO/IEC 17020 accreditation requirements.
    - C3PAOs shall not be authorized to conduct CMMC assessments until achieving CMMC Level 3 certification themselves for their unclassified networks and/or segments (internal and external) that store, process, and transmit CUI.
    - Require that all C3PAOs authorized to conduct CMMC assessments be subjected to quality assurance reviews to include but not limited to observations of their conduct and management of CMMC assessment processes.
2. Accredit C3PAOs in accordance with ISO/IEC 17020 and DoD requirements.
    - Require all C3PAOs achieve and maintain the ISO/IEC 17020 accreditation requirements within 27 months of registration.
3. Require C3PAOs to electronically submit pre-assessment material, final assessment reports and appropriate CMMC certificates to OUSD(A&S)/OCISO(A&S) CMMC Office via CMMC eMASS or an alternative DoD system.
4. The CMMC-AB will provide an up-to-date list of registered candidate C3PAOs, authorization and accreditation records and status. This data will include the dates associated with the authorization and accreditation of each C3PAO. This information will be stored by

the DoD in the CMMC eMASS or an alternative DoD system, using the format specified by the DoD.

5. Require C3PAOs to establish a formal process to address DIB contractor complaints and appeals, in accordance with ISO/IEC 17020, and submit investigation and decisions, to include dispute resolution results, to OUSD(A&S)/OCISO(A&S) CMMC Office via CMMC eMASS.
6. Require the C3PAO to agree that if it loses authorization or accreditation, that it must return or provide certification that it has destroyed all assessment related records in its possession.
7. Establish, maintain, and manage an up-to-date list of authorized and accredited C3PAOs on a publicly-accessible CMMC "Marketplace" website whose specific name and detailed function will be mutually agreed upon by the parties. The CMMC-AB shall provide a listing of these entities and their status to the DoD.
8. The CMMC-AB shall not publish nor change requirements for the authorization and accreditation of C3PAOs without the review and approval of the OUSD(A&S)/OCISO(A&S) CMMC Office.
9. In coordination with and after approval from the OUSD(A&S)/OCISO(A&S) CMMC Office, publish the current DoD and ISO/IEC accreditation requirements for C3PAOs in a downloadable document on the publicly-accessible CMMC "Marketplace" website.
10. Provide the DoD with information about the authorization and accreditation status of C3PAOs. Specifically, in response to reasonable requests for information pertaining to issues and to aggregate statistics, provide all responsive information; and in response to requests for other information regarding the status of C3PAO authorization and accreditation status, provide responsive information as mutually agreed to by the parties.
11. Provide inputs for supplemental guidance for assessors to the OUSD(A&S)/OCISO(A&S) CMMC Office. Participate and support coordination of these and other inputs through DoD-led Working Groups for consideration for inclusion into the CMMC Assessment Guides.

B. Authorization and Accreditation of CAICO

1. Authorize the CAICO to certify CMMC assessors and instructors, during the 24-month provisional period starting 31 October 2020 and ending 30 October 2022, only after verifying they have met all specified DoD requirements (to be provided to the CMMC-AB NLT 31 January 2021 via a bilateral modification and incorporation in the contract IAW Article III.B of the terms and conditions) with the exception of achieving the ISO/IEC 17024 accreditation requirements.
2. Accredit the CAICO in accordance with ISO/IEC 17024 and specified DoD requirements.
    a. Require the CAICO to achieve and maintain the ISO/IEC 17024 accreditation requirements within 25 months of registration.
3. Establish, maintain, and manage an up-to-date list of the authorized and accredited CAICO on a publicly-accessible CMMC "Marketplace" website whose specific name and detailed function will be mutually agreed upon by the parties. The CMMC-AB shall provide a listing of this entity and its status to the DoD.
4. The CMMC-AB will provide an up-to-date list of registered candidate assessors, training records, authorized assessors, and certified assessors, registered candidate instructors, authorized instructors, and certified instructors. This data will include the dates associated

with assessor or instructor training and the dates certification awards. The data will also include instructor affiliation with Licensed Training Providers and the modules they are certified to instruct. This information will be stored by the DoD in the CMMC eMASS or an alternative DoD system using the format specified by the DoD.

5. The CMMC-AB will not publish nor change requirements for the authorization and accreditation of the CAICO without review and approval by the OUSD(A&S)/OCISO(A&S) CMMC Office prior to implementation to ensure compliance with the CMMC Model, CMMC Assessment Guides and DoD policies.
6. In coordination with OUSD(A&S)/OCISO(A&S) CMMC Office, publish the current DoD accreditation requirements for the CAICO on the publicly-accessible CMMC "Marketplace" website.
7. Provide the DoD with information about the authorization and accreditation status of CACIO. Specifically, in response to reasonable requests for information pertaining to issues and to aggregate statistics, provide all responsive information; and in response to requests for other information regarding the status of CACIO authorization and accreditation status, provide responsive information as mutually agreed to by the parties.

C. Information Technology (IT) and Infrastructure

1. The CMMC-AB, C3PAOs, and the CAICO will not be allowed to store, process, handle, or transmit CUI on internal systems until those internal IT systems and/or networks meet CMMC Level ~~3~~2 and are certified by DoD assessors from the Defense Contracting Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).
2. The CMMC-AB shall not store, process, handle, or transmit CUI on any external non-DoD system until such external information system is certified by Government assessors from the DCMA to be CMMC Level ~~3~~2 compliant.
    - If the CMMC-AB uses an external cloud service provider to store, process, or transmit CUI, the CMMC-AB shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.
    - If the CMMC-AB uses an external cloud service provider, the CMMC-AB is responsible for addressing cybersecurity gaps that exist between the FedRAMP Moderate baseline and CMMC Level ~~3~~2.
    - If the CMMC-AB selects services from an external cloud service provider that has not been FedRAMP authorized, the CMMC-AB shall hire a Third Party Assessment Organization (3PAO) approved by the GSA FedRAMP Program Management Office to independently assess the external cloud service provider using the same assessment methodology and criteria established by GSA FedRAMP Program Management Office for a FedRAMP Moderate Baseline approval. The CMMC-AB will provide this assessment result to the DIBCAC in support of the CMMC Level ~~3~~2 assessment.
3. Require all C3PAO information systems (internal and external), including any assessment tools, that store, process, or transmit CUI, to be certified CMMC Level ~~3~~2 by DCMA DIBCAC assessors before conducting assessments and receiving authorization or accreditation from the CMMC-AB.

- If a C3PAO uses an external cloud service provider to store, process, or transmit CUI, the C3PAO shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.
- If a C3PAO selects services from an external cloud service provider that has not been FedRAMP authorized, the C3PAO shall hire a Third Party Assessment Organization (3PAO) approved by the GSA FedRAMP Program Management Office to independently assess the external cloud service provider using the same assessment methodology and criteria established by GSA FedRAMP Program Management Office for a FedRAMP Moderate Baseline approval. The C3PAO will provide this assessment result to the DIBCAC in support of the CMMC Level ~~3~~2 assessment.

4. Require all independent individual assessors, who are not employees of C3PAOs, to use IT, cloud, and cybersecurity services and end-point devices provided by the accredited C3PAO whom they are supporting and who has received a CMMC Level ~~3~~2 or higher certificate. Individual assessors are prohibited from using their own IT (to include internal and external cloud services) and end-point devices to store, process, handle, or transmit assessment reports and any other related information,
5. Designate CMMC-AB users who require access to the CMMC eMASS using CMMC Level ~~3~~2 certified IT. The DoD must approve and authenticate these designated individuals and may deny access in its sole discretion. If the Government denies access, it will provide the CMMC-AB with the reason for denial and acceptable modes of mitigation.

D. Security

1. Require individual assessors for Level 1, based in the US, and supporting the DoD, to be a U.S. person and have a favorably adjudicated Tier 1 suitability determination that results in no security clearance.
2. Require all Level 1 assessors, who are internationally based, to meet the equivalent of a favorably adjudicated Tier 1 suitability determination that results in no security clearance.
3. Require individual assessors for Level 2 or higher, based in the US, and supporting the DoD, to be U.S. Citizens and have a favorably adjudicated Tier 3 suitability determination that results in no security clearance.
4. Require all Level 2 or higher assessors, who are internationally-based, to meet the equivalent of a favorably adjudicated Tier 3 suitability determination that results in no security clearance.
5. Require all Level 1 C3PAOs' outsourced IT, managed service provider (MSP), and managed security service provider (MSSP) support organizations staff who view or handle assessment data, either electronically or physically, to be U.S. persons and undergo a suitability determination consistent with a favorably adjudicated Tier 1 suitability determination that results in no security clearance.
6. Require all Level 2 or higher C3PAOs' outsourced IT, MSP, and MSSP support organizations staff who view or handle assessment data, either electronically or physically to be U.S. Citizens and undergo a suitability determination consistent with a favorably adjudicated Tier 3 suitability determination that results in no security clearance.
7. The CMMC-AB shall require C3PAOs to provide proof of nationality of investors of the C3PAO, the identity of individual investors of the C3PAOs, business registration information

of the C3PAO, proof and validation of the source of funds of a foreign investment or foreign funds provided to the C3PAO, the ownership structure and identities of the board members and directors of the C3PAO. The CMMC-AB shall provide this information to the DoD prior to C3PAO accreditation and when requested. Risk decisions shall be made in accordance with the attached risk matrix and the CMMC-AB shall accept no entity with a risk factor greater than medium. In extenuating circumstances, a request for a waiver may be submitted with documented mitigation steps.

The CMMC-AB shall require certified CMMC assessors, who are employed or contracted by a C3PAO, to be citizens of the country where the C3PAO is physically located and can only assess contractors based in that country. The CMMC-AB cannot enter into any agreements with international entities without the approval of DoD.

E. Administrative

1. The OUSD(A&S)/OCISO(A) CMMC office and CMMC-AB mutually agree to protect and restrict CMMC related data or metrics for official business purposes and TO THE MAXIMUM EXTENT PRACTICABLE, ensure that data released publicly is coordinated prior to release. Both parties further agree to collaborate on CMMC program related strategic messaging to ensure alignment, and to maintain effective lines of communications between each other to facilitate program success.
2. The CMMC-AB will support DoD in establishing reciprocity and/or standard acceptance agreements with other entities for other cybersecurity standards (e.g. ISO 27001, GSA FedRAMP, DoD Standard Assessment Methodology, etc.) and shall implement processes and policies and include appropriate instruction for CMMC instructors and Certified CMMC assessors to credibly address and support such reciprocity and/or standard acceptance agreements.
3. The CMMC-AB shall establish and maintain appropriate and consistent communication channels with the Government regarding all CMMC-AB activities and shall support DoD-led Working Groups.
4. The CMMC-AB shall provide consistent and accurate monthly, quarterly and annual status update reports to the OUSD(A&S)/OCISO(A&S) CMMC Office, to include significant findings and C3PAO accreditation status, assessor certification status, and assessor training status.
5. The CMMC-AB shall participate in an annual review held by the OUSD(A&S)/OCISO(A&S) CMMC Office to determine adherence to the CMMC-AB's responsibilities as defined in this contract.
6. The CMMC-AB will not publish nor change requirements for CMMC assessors, lead assessors, assessment team members, assessment team size and composition, trainers, and instructors without the review and approval of the OUSD(A&S)/OCISO(A&S) CMMC Office.
7. Instill fairness, trust, and confidence in CMMC by overseeing and governming CMMC Ecosystem-wide adherence and fidelity to the CMMC Code of Professional Conduct and maintaining regular reporting on CMMC ethics and conflicts of interest concerns to the Department of Defense.

V. DoD Responsibilities:

OUSD(A&S)/OCISO(A&S) CMMC Office will conduct the following activities in the manner described below:

1. Retain oversight of the CMMC program to include the CMMC-AB.
2. Develop, update, maintain, and publish the CMMC Model, all CMMC Assessment Guides, and policies for the DoD implementation of CMMC framework.
3. Establish specified DoD requirements in addition to ISO/IEC 17020 for the authorization and accreditation of C3PAOs.
4. Establish specified DoD requirements in addition to ISO/IEC 17024 for the authorization and accreditation of the CAICO.
5. Establish specified DoD requirements for CMMC assessors, lead assessors, assessment team members, assessment team size and composition, trainers, and instructors.
6. Establish and maintain regular coordination with CMMC-AB to include weekly telecons to coordinate on current status, and a monthly meeting to exchange status updates and discuss plans to address mid-term to far-term issues or opportunities.
7. Provide a written and recordable Summary of Conclusions of key CMMC-AB meetings and coordinate approved and dated Summary of Conclusions with CMMC AB for concurrence within three 3 business days of meeting.
8. Coordinate and synchronize all CMMC model version releases with the CMMC-AB and the DIB SCC, to provide sufficient time for CMMC-AB to inform C3PAOs and the CAICO.
9. Coordinate and synchronize all CMMC Assessment Guides version releases with the CMMC-AB and the DIB SCC to provide sufficient time for CMMC-AB to inform the C3PAOs and the CAICO.
10. Provide the CMMC-AB with initial draft training material on CMMC background information, the CMMC Model, and CMMC Assessment Guides for use by the CMMC-AB as Government Furnished Information (GFI).
11. Establish and maintain the CMMC eMASS infrastructure and provide access to the CMMC-AB as GFI. Both parties agree to identify specific responsibilities, tasks, and Service Level Agreements requirements upon contract award.
12. Grant access to CMMC eMASS to select members of C3PAOs as GFI conditioned upon users meeting DoD requirements and procuring appropriate certificates.
13. Develop the data fields requirements and templates associated with the Assessment Reports for all C3PAOs and assessors.
14. Populate and keep current a list of DIB entities and their CMMC certification level in the CMMC eMASS and Supplier Performance Risk System.
15. Communicate the requirement to achieve CMMC certification to companies in the DIB.
16. Establish reciprocity and/or standard acceptance agreements with other entities for other cybersecurity standards (e.g. ISO 27001, GSA, FedRAMP, DoD Standard Assessment Methodology, etc.). Collaborate with and seek input from the CMMC-AB and the DIB SCC in the process of establishing reciprocity and/or standard acceptance agreements.

17. Provide factual information to the CMMC-AB 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).
18. Identify programs to assist small businesses with the preparation for achieving CMMC requirements and successfully completing CMMC assessments.
19. Establish and maintain open communication channels with the CMMC-AB to include CMMC-AB participation in DoD-led Working Groups where appropriate.
20. Conduct a quarterly review with the CMMC-AB Board of Directors to assess the parties' alignment with the understandings set forth in this contract and review the annual report from the CMMC-AB.
21. Sponsor and fund Tier 3 suitability determinations for the CMMC-AB staff.
22. Sponsor and fund Tier 3 suitability determinations that result in no security clearance for C3PAO assessors conducting CMMC Level 2 -5 assessments.
23. Sponsor and fund Tier 3 suitability determinations that result in no security clearance for outsourced support IT, MSP, and MSSP staff for CMMC-AB and C3PAOs conducting Level 2-5 assessments.
24. Sponsor and fund Tier 1 suitability determinations that result in no security clearance for CMMC assessors conducting CMMC Level 1 assessments.
25. Sponsor and fund Tier 1 suitability determinations that result in no security clearance for outsourced support IT, MSP, and MSSP staff for C3PAOs conducting Level 1 assessments.
26. The DoD shall ensure that an alternative DoD system is available for temporary use in the even that CMMC eMASS is not operationally available prior to the conduct of CMMC assessments by authorized C3PAOs. To the maximum extent possible and practical, the DoD will respond to CMMC-AB requests within 2 weeks.
~~26.~~27. Review and approve the CMMC-AB's Conflict of Interest Policy and the CMMC Code of Professional Conduct, as well as any subsequent updates or revisions to said documents.

DCMA DIBCAC assessors will conduct the following activities in the manner described below:

1. Complete training and obtain certification from the CAICO.
2. Complete CMMC training during the provisional 24-month period prior to conducting CMMC assessments.
3. Conduct CMMC Level 3 assessments of the CMMC-AB information systems that process, store, and/or transmit CUI. DCMA DIBCAC may request augmentation from other DoD assessors on an-as needed basis.
4. Conduct CMMC assessments for candidate C3PAOs. DCMA DIBCAC may request augmentation from other DoD assessors on an-as needed basis.

VI. Performance Objectives:

Required Performance	Performance Standard	Maximum Allowable Degree of	Method of Surveillance

		Deviation Requirement	
Provide a Comprehensive Plan / Roadmap for achieving compliance with ISO/IEC 17011 standards within no more than 2 years. As part of this plan, include a detailed risk mitigation plan for any and all identified potential conflicts of interest that may pose a risk to compliance with ISO/IEC 17011. This plan must specify the establishment of the CAICO which is separate and independent from the CMMC-AB and will meet all ISO/IEC 17024 requirements.	- Completed self-assessment against the ISO/IEC 17011 standard in 1QFY21 - Identify executable steps and realistic timelines to eliminate potential conflicts of interest between (i) accreditation and DIB CMMC certification activities; and (ii) accreditation and assessor and instructor certification. 2QFY21.	1 month	OUSD(A&S)/OCISO(A&S) CMMC Office review and approval of the Transition Plan / Roadmap.
Become an approved associate member of the InterAmerican Accreditation Cooperation (IAAC) and remain in good standing.	October 31, 2021	1 month	OUSD(A&S)/OCISO(A&S) CMMC Office review of Membership status during monthly CMMC-AB reviews.
Achieve conformity with ISO/IEC 17011 to support performing accreditation body functions for ISO/IEC 17020 and ISO/IEC 17024	~~October 31, 2022 (or 24 months after contract signature)~~April 30, 2023	1 month	Independent Peer Evaluation that verifies full compliance of all ISO/IEC 17011 requirements through peer review(s) by representatives from ISO / IEC 17011 Accreditation Bodies IAW ISO/CASCO
Conduct management reviews IAW ISO/IEC 17011 para 9.8 and provide results to the DoD CMMC program office. The annual review must include the results of the latest self-assessment and any independent, peer reviews not previously provided to the	Annual (to be scheduled by mutual agreement)	N/A	OUSD(A&S)/OCISO(A&S) CMMC Office annual review of CMMC-AB

OUSD(A&S)/OCISO(A&S) CMMC Office.			
Become an approved full member of InterAmerican Accreditation Cooperation (IAAC) after achieving ISO/IEC 17011 compliance and shall remain in good standing.	October 31, 2023 (or 36 months after contract signature)	1 month	OUSD(A&S)/OCISO(A&S) CMMC Office review of Membership status during monthly reviews.

VII. Deliverables:

Both parties agree that there are variables that may impact the threshold and objective delivery dates established below, and agree to reassess for reasonable consideration and relief as circumstances dictate. To be delivered to the COR for the OUSD(A&S)/ OCISO(A&S) CMMC Office:

1. ISO/IEC 17011 Compliance Roadmap and Plan that identify key planned milestones to include, but not limited to, membership in IAAC, transitioning training to an independent certification body, development of a revised business plan, dates for conducting self-assessment, peer reviews and achieving compliance. Distribution: Please submit to the COR, PMO, and KO via email.
   Threshold 2nd Quarter FY2021 Objective 1st Quarter FY2021
2. Updates and progress on ISO/IEC 17011 Compliance Roadmap and Plan to on a monthly basis. Distribution: Please submit to the COR, PMO, and KO via email.
3. Results of all ISO/IEC 17011 self-assessments, independent assessments, and peer reviews. Distribution: Please submit to the COR, PMO, and KO via email.
4. List of all current and planned subcontracts, on a monthly basis, that support the CMMC-AB in their functions as an accreditation body as well as those subcontracts that support training, assessment and consulting related activities. Distribution: Please submit to the COR, PMO, and KO via email.
5. CMMC-AB Conflict of Interest Policy and CMMC Code of Professional Conduct. The former must include specific language requiring the disclosure of potential conflicts-of-interest (COI) by CMMC-AB professional staff and Board directors and the associated mitigation policies and procedures. The latter must include specific language prohibiting any C3PAO, CMMC Certified Professional (CCP), or CMMC Certified Assessor (CCA) from participating in any CMMC certification Assessment of DIB companies (i.e., organizations seeking certification) to whom they provided paid consulting services within the previous two (2) years. The Department of Defense will review and approve both documents as well as any subsequent revisions therein. ~~Comprehensive Conflict of Interest (COI) and Ethics Plan: inclusive of CMMC-AB, C3PAOs, individual assessors, trainers, and others for DoD review and comment. This includes policy that prohibits any individual and C3PAO from providing paid consulting services and assessments to the same DIB contractor. This also includes policy that prohibits any CMMC-AB member or the CMMC-AB from having a conflict of interest in the execution of its responsibilities. Any proposed changes must be coordinated with the USD(A&S)/OCISO(A&S) CMMC Office prior to implementation.~~ Distribution: Please submit to the COR, PMO, and KO via email.

Threshold 1st Quarter FY2021

6. Communications Plan: NLT January 31 2021, Provide OUSD(A&S)/ OCISO(A&S) CMMC Office with a strategic CMMC-AB communications strategy that sets forth the CMMC-AB's approach for updating the CMMC-AB and CMMC "Marketplace" website(s) and provide updated plan when the plan is changed and notify the OUSD(A&S)/OCISO(A&S) CMMC Office of the changes during the weekly sync. Distribution: Please submit to the COR, PMO, and KO via email.
7. Quality Control Plan: inclusive of key CMMC-AB duties to include but not limited to the authorization and accreditation of C3PAOs and the CAICO, as well as the interim duties associated with training (i.e. training material development, instruction, examination, etc.).
8. Threshold 1st Quarter FY2021Change Control Procedures: The established procedures used by the CMMC-AB to process Government specified changes prior to implementation in training and testing content. The procedures shall include the CMMC-AB providing the results of the change control review, to include but not limited to, the impact, schedule, and risk analysis within 2 weeks of a Government's change request submission to the CMMC-AB. Distribution: Please submit to the COR, PMO, and KO via email.

   Threshold 1st Quarter FY2021
9. Training – Training of candidate assessors for CMMC up to Level 3 shall start:

   Threshold 2nd Quarter FY2021
10. Training – Training of candidate assessors for CMMC Levels 4 & 5 shall start:

    Threshold 4th Quarter FY2021

    Objective 3rd Quarter FY2021

    - Contingent on when DoD provides the appropriate assessment guide training materials
11. Training Targets – Year 1: 360 assessors trained for up to CMMC Level 3:

    Threshold 4rd Quarter FY2021

    Objective 3rd Quarter FY2021
12. Training Targets – Year 2: 1500 assessors trained:

    Threshold 2nd Quarter FY2022

    Objective 1st Quarter FY2022 with consistent progress throughout the remainder of the contract.
13. Training Targets – Year 1: 15 assessors trained for CMMC Level 4 & 5

    Threshold 4th Quarter FY2021

    Objective 3rd Quarter FY2021
14. Training curricula (training material, videos, documents, lesson plans, and instructor notes) and examinations, test bank questions and answers. Distribution: Please submit to the COR, PMO, and KO via Safe.

    Threshold: Finalized products prior to implementation
15. Monthly status reports must be delivered the 10th day of every month to include:
    - Name of all registered, authorized and accredited C3PAOs

- Name and affiliation of all registered, trained, and certified assessors by level
- Status of Quality Assurance assessments conducted on C3PAOs and certified assessors
- Number of assessors who failed training, by level and identifying the failure areas
- Status of the authorization and accreditation of the CAICO
- Name and affiliation of all registered and trained instructors
- Training statistics to include number of assessors trained per training organization, average exam score and failure rates per training class by organization and instructor(s).

16. Quarterly status report documenting the metrics provided in deliverable Number 14 for each quarter of a fiscal year. Delivery Time: 30 days after each quarter. Distribution: Please submit to the COR, PMO, and KO via Safe.
17. Annual status report documenting the metrics provided in deliverable Number 14 for the fiscal year. Delivery Time: October 31, every year. Distribution: Please submit to the COR, PMO, and KO via Safe.
18. Transition out plan – Upon request, provide a transition out plan within 30 calendar days, for transfer of operations to another body in the event this contract is terminated. Distribution: Please submit to the COR, PMO, and KO via Safe.

Deliverables 1-8 must be provided to the COR, PMO, and KO via email. Deliverables 14-18 must be provided through DoD's Secure Access File Exchange (SAFE) at https://safe.apps.mil/.