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 assesments, 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 sytem, 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) High 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 High 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 High 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) High 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 High 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	- Completed self-assessment against the ISO/IEC 17011 standard in 1QFY21 - Identify executable steps and realistic timelines to eliminate potential conflicts of	1 month	OUSD(A&S)/OCISO(A&S) CMMC Office review and approval of the Transition Plan / Roadmap.

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.	interest between (i) accreditation and DIB CMMC certification activities; and (ii) accreditation and 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.

   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.
3. Results of all ISO/IEC 17011 self-assessments, independent assessments, and peer reviews.
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.
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 OUSD(A&S)/OCISO(A&S) CMMC Office prior to implementation.

   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.

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 reveiw, 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.

   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 3nd 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.

    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.
17. Annual status report documenting the metrics provided in deliverable number 14 for the fiscal year. Delivery Time: October 31, every year.
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.