developed by a CMMC training organization approved by the CAICO in all CMMC certification courses.

(iii) *Ethics policy*. The Ethics policy shall:

(A) Require CMMC Ecosystem members to report to the Accreditation Body within 30 days of convictions, guilty pleas, or no contest pleas to crimes of fraud, larceny, embezzlement, misappropriation of funds, misrepresentation, perjury, false swearing, conspiracy to conceal, or a similar offense in any legal proceeding, civil or criminal, whether or not in connection with activities that relate to carrying out their role in the CMMC Ecosystem.

(B) Prohibit harassment or discrimination by CMMC Ecosystem members in all interactions with individuals whom they encounter in connection with their roles in the CMMC Ecosystem.

(C) Require CMMC Ecosystem members to have and maintain a satisfactory record of integrity and business ethics.

§ 170.9 CMMC Third-Party Assessment Organizations (C3PAOs).

(a) *Roles and responsibilities*. C3PAOs are organizations that are responsible for conducting Level 2 certification assessments and issuing Certificates of CMMC Status to OSCs based on the results. C3PAOs must be accredited or authorized by the Accreditation Body in accordance with the requirements set forth.

(b) *Requirements*. C3PAOs shall:

(1) Obtain authorization or accreditation from the Accreditation Body in accordance with §170.8(b)(3)(i) and (ii).

(2) Comply with the Accreditation Body policies for Conflict of Interest, Code of Professional Conduct, and Ethics set forth in §170.8(b)(17); and achieve and maintain compliance with ISO/IEC 17020:2012(E) (incorporated by reference, see §170.2) within 27 months of authorization.

(3) Require all C3PAO company personnel participating in the Level 2 certification assessment process to complete a Tier 3 background investigation resulting in a determination of national security eligibility. This includes the CMMC Assessment Team and the quality assurance individual. This Tier 3 background investigation will not result in a security clearance and is not being executed for the purpose of government employment. The Tier 3 background investigation is initiated using the Standard Form (SF) 86 (*www.gsa.gov/reference/forms/questionnaire-for-national-security-positions*). These positions are designated as noncritical sensitive with a risk designation of ''Moderate Risk'' in accordance with 5 CFR 1400.201(b) and (d) and the investigative requirements of 5 CFR 731.106(c)(2).

(4) Require all C3PAO company personnel participating in the Level 2 certification assessment process who are not eligible to obtain a Tier 3 background investigation to meet the equivalent of a favorably adjudicated Tier 3 background investigation. DoD will determine the Tier 3 background investigation equivalence for use with the CMMC Program only.

(5) Comply with Foreign Ownership, Control or Influence (FOCI) by:

(i) Completing and submitting Standard Form (SF) 328 (*www.gsa.gov/reference/forms/certificate-pertaining-to-foreign-interests*), *Certificate Pertaining to Foreign Interests*, upon request from DCSA and undergo a National Security Review with regards to the protection of controlled unclassified information based on the factors identified in 32 CFR 117.11(b) using the procedures outlined in 32 CFR 117.11(c).

(ii) Receiving a non-disqualifying eligibility determination from the CMMC PMO resulting from the FOCI risk assessment in order to proceed to a DCMA DIBCAC CMMC Level 2 assessment, as part of the authorization and accreditation process set forth in paragraph (b)(6) of this section.

(iii) Reporting any change to the information provided on its SF 328 by resubmitting the SF 328 to DCSA within 15 business days of the change being effective. A disqualifying eligibility determination, based on the results of the change, will result in the C3PAO losing its authorization or accreditation.

(6) Undergo a Level 2 certification assessment meeting all requirements for a Final Level 2 (C3PAO) in accordance with the procedures specified in

§170.17(a)(1) and (c), with the following exceptions:

(i) The assessment will be conducted by DCMA DIBCAC.

(ii) The assessment will not result in a CMMC Status of Level 2 (C3PAO) nor receive a Certificate of CMMC Status.

(7) Provide all documentation and records in English.

(8) Submit pre-assessment and planning material, final assessment reports, and CMMC certificates of assessment into the CMMC instantiation of eMASS.

(9) Unless disposition is otherwise authorized by the CMMC PMO, maintain all assessment related records for a period of six (6) years. Such records include any materials generated by the C3PAO in the course of an assessment, any working papers generated from Level 2 certification assessments; and materials relating to monitoring, education, training, technical knowledge, skills, experience, and authorization of all personnel involved in assessment activities; contractual agreements with OSCs; and organizations for whom consulting services were provided.

(10) Provide any requested audit information, including any out-of-cycle from ISO/IEC 17020:2012(E) requirements, to the Accreditation Body.

(11) Ensure that all personally identifiable information (PII) is encrypted and protected in all C3PAO information systems and databases.

(12) Meet the requirements for Assessment Team composition. An Assessment Team must include at least two people: a Lead CCA, as defined in §170.11(b)(10), and at least one other CCA. Additional CCAs and CCPs may also participate on an Assessment Team.

(13) Implement a quality assurance function that ensures the accuracy and completeness of assessment data prior to upload into the CMMC instantiation of eMASS. Any individual fulfilling the quality assurance function must be a CCA and cannot be a member of an Assessment Team for which they are performing a quality assurance role. A quality assurance individual shall manage the C3PAO's quality assurance reviews as defined in paragraph (b)(14) of this section and the appeals process as required by paragraphs (b)(19) and (20) of this section and in accordance with ISO/IEC 17020:2012(E) (incorporated by reference, see §170.2) and ISO/IEC 17011:2017(E) (incorporated by reference, see §170.2).

(14) Conduct quality assurance reviews for each assessment, including observations of the Assessment Team's conduct and management of CMMC assessment processes.

(15) Ensure that all Level 2 certification assessment activities are performed on the information system within the CMMC Assessment Scope.

(16) Maintain all facilities, personnel, and equipment involved in CMMC activities that are in scope of their Level 2 certification assessment and comply with all security requirements and procedures as prescribed by the Accreditation Body.

(17) Ensure that all assessment data and information uploaded into the CMMC instantiation of eMASS assessment data is compliant with the CMMC assessment data standard as set forth in eMASS CMMC Assessment Import Templates on the CMMC eMASS website: *https://cmmc.emass.apps.mil*. This system is accessible only to authorized users.

(18) Issue Certificates of CMMC Status to OSCs in accordance with the Level 2 certification assessment requirements set forth in §170.17, that include, at a minimum, all industry CAGE codes associated with the information systems addressed by the CMMC Assessment Scope, the C3PAO name, assessment unique identifier, the OSC name, and the CMMC Status date and level.

(19) Address all OSC appeals arising from Level 2 certification assessment activities. If the OSC or C3PAO is not satisfied with the result of the appeal either the OSC or the C3PAO can elevate the matter to the Accreditation Body for final determination.

(20) Submit assessment appeals, review records, and decision results of assessment appeals to DoD using the CMMC instantiation of eMASS.