POSITION PAPER

Against the Practice of C3PAO-Conducted Mock Assessments

An Analysis Under ISO/IEC 17020, ISO 17000, and the CMMC Assessment Process

March 2026

Executive Summary

This paper presents the argument that CMMC Third-Party Assessor Organizations (C3PAOs) should not conduct mock assessments for Organizations Seeking Certification (OSCs) that they subsequently assess in a formal certification capacity. This practice creates fundamental conflicts with the impartiality requirements of ISO/IEC 17020:2012, undermines the conformity assessment classification framework established by ISO 17000:2020, compromises the evidentiary integrity of formal assessments, and creates an information asymmetry that defeats the regulatory intent of the CMMC program.

1. The Impartiality Imperative Under ISO/IEC 17020

C3PAOs operating within the CMMC ecosystem are accredited as inspection bodies under ISO/IEC 17020:2012. The standard's impartiality requirements are not discretionary guidance—they are foundational conditions for accreditation. The following clauses are directly implicated by the mock-to-formal assessment pipeline.

1.1 Identification of Threats to Impartiality (Clause 4.1.4)

ISO/IEC 17020:2012, Clause 4.1.4 requires the inspection body to "identify risks to its impartiality on an ongoing basis." The clause explicitly encompasses risks arising from the body's activities, its relationships, and the relationships of its personnel. When a C3PAO conducts a mock assessment, it enters into a collaborative, advisory relationship with the OSC. The C3PAO identifies gaps, provides remediation guidance, and develops a shared understanding of the environment's deficiencies. This relationship constitutes a textbook threat to impartiality that must be identified and managed under Clause 4.1.4.

1.2 Elimination or Minimization of Risk (Clause 4.1.5)

Clause 4.1.5 requires that once a risk to impartiality is identified, the inspection body must demonstrate how it eliminates or minimizes that risk. In the case of mock-then-certify arrangements, the self-review threat is inherent and unmanageable. The C3PAO cannot meaningfully claim independence when evaluating remediation efforts that were

undertaken in direct response to its own prior guidance. No organizational control, personnel rotation, or procedural safeguard can fully eliminate the cognitive and institutional bias created by having previously guided the OSC toward a desired outcome.

1.3 Prohibition on Consultancy (Clause 4.1.6)

Clause 4.1.6 addresses the provision of consultancy services by the inspection body. The critical question is whether a mock assessment constitutes consultancy. When a C3PAO conducts a mock assessment that involves identifying deficiencies and providing remediation guidance, it is performing a function that is functionally indistinguishable from consulting—regardless of how the engagement is labeled. The ISO framework is concerned with the substance of activities, not their labels. A “mock assessment” that tells an OSC what to fix and how to present its evidence is advisory work by any reasonable definition.

This directly parallels the existing CMMC Assessment Process (CAP) prohibition against an organization serving as both a Registered Provider Organization (RPO) and a C3PAO to the same client. The mock assessment construct creates the same conflict through a different mechanism.

2. The Conformity Assessment Classification Problem

ISO 17000:2020, Clause 4.3 establishes three types of conformity assessment activities based on who performs them. Analyzing the mock assessment under this framework reveals an irreconcilable classification problem.

2.1 The Mock Assessment as a Type 2 Activity

Under ISO 17000:2020, a second-party (Type 2) conformity assessment activity is one performed by a person or body with a “user interest” in the object. When a C3PAO conducts a mock assessment, it is not acting in its independent third-party capacity. It has a commercial interest in the client succeeding, in the engagement proceeding to formal assessment, and in the relationship continuing. These constitute “user interests” under the standard’s definition. The mock assessment is therefore, by its nature, a Type 2 activity.

2.2 The Classification Trap

Accepting that the mock is a Type 2 activity creates a logical trap for any argument favoring evidence bridging. If the mock is a Type 2 activity, the C3PAO has formally operated without independence during evidence collection. Evidence collected while operating as an interested party is, by definition, not impartially gathered under ISO/IEC 17020:2012, Clause 4.1.2. Such evidence cannot satisfy the evidentiary requirements of a Type 3 (third-party) determination.

Conversely, if one argues the mock is itself a Type 3 activity, then the C3PAO has conducted a formal independent assessment that resulted in findings. The question then becomes: why did this assessment not produce a certification determination? And why are the negative findings from this assessment not visible to the government as the relying party?

The entire purpose of distinguishing Types 1, 2, and 3 in ISO 17000 is that they carry different levels of confidence. Type 3 carries the highest confidence precisely because of independence. Bridging Type 2 evidence into a Type 3 conclusion undermines the classification system the standard establishes.

3. Evidentiary Integrity

A central argument advanced in favor of mock-to-formal pipelines is that evidence collected during the mock can be reused without reassessment, bridging the mock data to the final assessment data. This argument fails under scrutiny.

3.1 Validity of Inspection Results (Clause 7.1.8)

ISO/IEC 17020:2012, Clause 7.1.8 requires the inspection body to have procedures ensuring the validity of its inspection results. Evidence gathered in a non-independent, advisory context and subsequently carried into a formal assessment raises fundamental validity questions. The conditions under which the evidence was collected—collaborative, guided, advisory—are materially different from the conditions required for an independent third-party assessment. The provenance of the evidence is compromised.

3.2 Independence of Selection (ISO 17000:2020, Clause 6.1)

ISO 17000:2020, Clause 6.1, addressing selection—the process of choosing what gets assessed and how—presupposes that the conformity assessment body is making those decisions independently. If the mock assessment has already shaped what evidence exists and how it was prepared, the C3PAO's selection process in the formal assessment is tainted. The assessor is not independently sampling; they are confirming their own prior work. This is the self-review threat in its most explicit form.

3.3 The Determination Function (ISO 17000:2020, Clause 7.2)

ISO 17000:2020, Clause 7.2, on determination—the activity of ascertaining conformity—requires that the basis for the determination be sound. Evidence collected under Type 2 conditions does not meet the evidentiary standard required for a Type 3 determination. The bridging of evidence across engagement types conflates two fundamentally different levels of assurance.

4. Information Asymmetry and Regulatory Intent

Perhaps the most consequential argument against mock assessments concerns the information asymmetry they create between the assessment ecosystem and the government as the ultimate relying party.

4.1 The Government's Interest in Failure Data

There is a material difference between two states: (1) an OSC that has not yet been assessed, which is a neutral status representing an unevaluated risk; and (2) an OSC that was assessed and found nonconforming, which is an affirmative finding representing a known, evaluated risk. The government has a legitimate and compelling interest in distinguishing between these two states. An OSC that attempted and failed a third-party assessment represents an entity whose controls have been independently examined and found insufficient to protect Controlled Unclassified Information (CUI). This is materially different from an entity that simply has not been evaluated.

4.2 Mock Assessments as a Concealment Mechanism

If a C3PAO conducts a mock that is functionally identical to a formal assessment—same evidence collection, same evaluation methodology, same assessment team—but the negative result is not reported because the engagement is labeled a "mock," then the mock construct functions as a mechanism for concealing nonconformity findings from the government. The OSC can fail repeatedly in mock engagements, receive coaching on remediation, and only enter the formal record when success is assured. The government never sees the failures.

4.3 Undermining the Purpose of Third-Party Assessment

Under ISO 17000:2020, Clause 7, the determination and review functions exist specifically to produce reliable conformity information for decision-makers. The Department of Defense, as the ultimate relying party in the CMMC ecosystem, is the primary consumer of that information. The CMMC program, codified in 32 CFR Part 170, exists to provide the DoD with assurance about contractor cybersecurity posture. A process that allows an OSC to quietly fail and retry without that failure being visible to the government circumvents the regulatory intent of requiring third-party assessment in the first place.

5. The Existing RPO/C3PAO Prohibition as Precedent

The CMMC Assessment Process (CAP) already prohibits an organization from serving as both a Registered Provider Organization (RPO) and a C3PAO to the same client. This prohibition recognizes that consulting on CMMC readiness and then assessing the results of that consulting creates an unmanageable conflict of interest. The mock assessment construct creates an identical conflict through a different label. The RPO provides readiness guidance; the mock assessment provides readiness guidance. The RPO identifies gaps and advises on remediation; the mock assessment identifies gaps and advises on remediation. The only distinction is the name of the engagement.

If the CAP's RPO/C3PAO prohibition is sound—and the ISO standards strongly support its soundness—then permitting mock assessments by C3PAOs creates an inconsistency in the framework that allows the same conflict to persist under a different label.

6. Summary of ISO Citations

Standard / Clause	Relevance
ISO/IEC 17020:2012, Cl. 4.1.2	Impartiality throughout inspection activities
ISO/IEC 17020:2012, Cl. 4.1.4	Ongoing identification of risks to impartiality
ISO/IEC 17020:2012, Cl. 4.1.5	Demonstration of risk elimination or minimization
ISO/IEC 17020:2012, Cl. 4.1.6	Prohibition on consultancy compromising impartiality
ISO/IEC 17020:2012, Cl. 7.1	Inspection methods and procedures
ISO/IEC 17020:2012, Cl. 7.1.8	Validity of inspection results
ISO 17000:2020, Cl. 4.2	Classification of first-, second-, third-party activities
ISO 17000:2020, Cl. 4.3	Definition of conformity assessment types
ISO 17000:2020, Cl. 6.1	Independence of selection in conformity assessment
ISO 17000:2020, Cl. 7.2	Soundness of determination basis
ISO 17000:2020, Cl. 7	Determination and review functions for decision-makers
ISO 17000:2020, Cl. 8.1–8.2	Impartiality and freedom from conflicts of interest

7. Conclusion

The practice of C3PAOs conducting mock assessments for clients they subsequently certify is incompatible with the impartiality requirements of ISO/IEC 17020:2012, the conformity assessment classification framework of ISO 17000:2020, and the regulatory intent of the CMMC program under 32 CFR Part 170. The mock assessment construct creates the same advisory-then-assessment conflict that the CAP's RPO/C3PAO prohibition was designed to prevent, merely under a different label.

Furthermore, the practice introduces an information asymmetry that undermines the government's ability to distinguish between unevaluated contractors and contractors whose controls have been independently examined and found deficient. This asymmetry defeats the fundamental purpose of requiring third-party assessment in the CMMC ecosystem.

C3PAOs seeking to maintain compliance with ISO/IEC 17020 and their accreditation obligations should refrain from conducting mock assessments for any OSC they intend to formally assess. The CMMC ecosystem should consider formalizing this prohibition to maintain consistency with the existing RPO/C3PAO separation requirement and to preserve the integrity of the conformity assessment framework upon which the program relies.