C3PAO
STAKEHOLDER FORUM

August 27, 2022

CMMC Assessment Process

C3PAO Forum Comments

DISCLAIMER

The C3PAO Stakeholder Forum is an industry group of C3PAOs. The group is formed from C3PAOs and aspiring C3PAOs; it is open to all CyberAB Marketplace C3PAOs and confirmed C3PAO applicants. The mission is to advance the CMMC assessor and C3PAO input, participation, and consensus within the CMMC ecosystem. This includes advocating for policies, sharing perspectives and working alongside the DoD, CyberAB, Organizations Seeking Certification (OSC) and other stakeholders to advance the mission of CMMC, which broadly is to increase the cyber posture of the Defense Industrial Base. The C3PAO Stakeholder Forum's participation is voluntary and those individuals that participate do so of their own volition and without compensation. The views of the board and the C3PAO Stakeholder Forum are not necessarily those of each member or their respective companies. The DoD, and where delegated by the DoD to the CyberAB, are the ultimate authority with regard to CMMC. Any guidance contained within is not authoritative and if found in conflict with DoD guidance should be considered subordinate. We simply seek to share this guidance to help advance the conversations and drive consistency among the industry.

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

To Matt Travis, et. al,

Below you will find our combined feedback on the draft CMMC Assessment Procedure document. As a key group of stakeholders for the success of the CMMC program, we respectfully submit our feedback, concerns, and recommendations for your consideration.

Our feedback as a group is based on the following priorities:

- Reducing Cost of Assessment
- Reducing Complexity
- Increasing Executability
- Ensuring Consistency
- Reducing Legal Liability

PURPOSE

The purpose of this document is to collectively provide feedback in response to the Cyber- AB's request for comments regarding the recently release daft of the CMMC Assessment Process. The members of the C3PAO Forum have discussed the CAP over the past three weeks and propose the following changes.

COMMENTS

1. ECSP(CSP) vs ESP(MSP/MSSP)

- ECSP – External Cloud Service Provider
- CSP – Cloud Service Provider
- ESP – External Service Provider
- MSP – Managed Service Provider
- MSSP – Managed Security Service Provider

The CAP and process must not combine the two terms (ECSP and ESP). Requiring a defense contractor to use a CSP that is certified to the FedRAMP Moderate standard to store, process, or transmit CUI already exists through

DFARS 252.204-7012. Lumping the two very different types of service providers together creates an impossible and unreasonable expectation. The requirement exceeds the CyberAB legal authority by extending FEDRAMP requirements to ESP/MSP/MSSP.

Assessments should be conducted only according to the applicable controls and assessment objectives of NIST SP 800-171A.

It is apparent that the CAP does not appropriately address what ESP/MSPs/MSSPs do, the services they provide to the DIB, and the implications of the current requirements and expectations of the scoping guide and the assessment process.

Please reference the inheritancerecommendations previously submitted by the C3PAO Stakeholder Forum. This paper speaks to this specific issue and provides recommendations.

See: https://www.c3paoforum.org/wp-content/uploads/2022/05/Position-Evaluating-inheritable-practices-by-providers_public-1.pdf

2. ASSESSMENT PROCESS EXPANSION

The CAP should not expand on the assessment process already outlined in the assessment guide. In the current draft the CAP does expand on the assessment process in the following sections:

Pre-Assessment

It is our understanding that the pre-assessment begins after the signing of the contract with the OSC. Other than initial engagement conversations, no work starts until a contract is signed. This needs to be stated/clarified to avoid OSC confusion and incorrect expectations on when the work can begin.

Appeals Process

Currently, the CAP sets the appeals process to be strictly handled by the original C3PAO. We firmly believe that after the initial appeals process through the C3PAO, there must be an independent third-party appeals process ***in accordance with applicable ISO standards*** and to provide an opportunity for escalation. The appeals process should be expanded so that after an appeal to the C3PAO, the next level of the appeal goes to the Cyber-AB or another independent third party as determined by the Cyber-AB.

3. CONFLICTS OF INTEREST, LEGAL LIABILITY

The Cyber-AB should develop a process to help indemnify the C3PAO from liability for an OSC suing the C3PAO based on disagreeing with the assessment results.

The appeals process should escalate from the C3PAO (initial appeal) up to the Cyber-AB, who should have the final authority to manage, address, and resolve disputes.

4. ARCHIVING AND DESTRUCTION OF OSC DATA

Page 7, "Confirmation of Destruction of OSC Data" implies that expressed written consent from the OSC would allow the C3PAO to keep/maintain an archive of the OSCs assessment documents. In section 1.5.4, it specifically states "It is a violation of the CMMC Code of Professional Conduct (and of the *CMMC Assessment Process*) for a C3PAO to retain OSC proprietary information past the conclusion of the C3PAO-OSC engagement." This is a point of contention for the C3PAO community that must be clarified. We believe that it should be in our contract with the OSC that the OSC agrees to allow the C3PAO to archive/maintain the assessment data. It is our firm position that for integrity and liability, this data should be maintained, along with the hashing.

Without being able to archive and maintain all the OSCs assessment data, the effort necessary for C3PAOs to document and capture everything necessary to address our liability will drive the cost of an assessment up, and risk C3PAOs inability to defend our assessments. There are more effective ways to provide security and protection of the OSCs data.

We recommend changing the wording regarding the professional code of conduct to state that it can be done with the OSCs written permission, and the data would be protected according to the contract with the OSC.

Optionally, the archive of all the assessment documentation would be maintained either by the Cyber AB or the DoD in the CMMC eMASS or other repository.

5. CUI AND THE C3PAO ASSESSMENT

Based on our understanding of what constitutes CUI and the assessment process, we firmly agree that the artifacts and evidence that will be required in order to prove compliance should not contain any CUI. C3PAOs are not authorized to have access to the CUI that an OSC would possess. Any accidental exposure of CUI is the responsibility of the OSC.

CLOSING

An approval vote was conducted by the C3PAO Forum. The following members have affirmed the collective feedback provided above:

Kevin Wheeler – InfoDefense
Cathy Sands – Omnistruct
Nick DeLena – DGC
Kelly Kendall – KNC Strategic
Thomas Nohs – DataSoftNow
Amira Armond – Kieri Solutions
Chris Silvers – CG Silvers
Leighton Johnson – ISFMT
Bill Nelson – Smithers
Tony Buenger – SecureStrux
Scott Singer – CyberNINES
Rick Verrill – Excentium
David Corrigan – APS Global
Tony Bai – A-LIGN
Debbie Hunt – iPower
Brian Brethen – La Jolla Logic
Tim Kiggins – Global SecOps
Ben Taylors – The New IT
Consuela Blount – Sentar
Nathan Kennedy – G2OPS
Melvin Kendall – Vaultes
Jason Luke – TechLock
Kyle Lai – KLC Consulting
Josh Chin – Net Force

Thank you for your consideration and efforts to improve the CAP. We are happy to discuss any of these points with you.

Warm regards,

The CMMC C3PAO Stakeholders Forum