POSITION PAPER SERIES

Assign responsibility for technical clarifications

September 30, 2021

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 CMMC-AB 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 include advocating for policies, sharing perspectives and working alongside the DoD, CMMC-AB, Organizations seeking certification 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 CMMC-AB, 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. To the extent that subsequent guidance is published by the DoD or similar authorities, this document will be revised.

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.

PURPOSE

To establish responsibility for authoritative guidance to assessors and C3PAOs which meets the following criteria:

1) is responsive to assessment teams in the midst of assessments

2) is applicable to other assessments and organizations facing the same situation

3) is publicly referenceable

DISCUSSION

- Problem Statement

The DFARS Cyber FAQ is an excellent resource for DFARS 252.204-7012 technical clarifications. However, even this document leaves large gaps for personal interpretation. This has not been an urgent issue until now because defense contractors were not subject to an outside opinion about their implementations.

The DIB is already making major changes to their infrastructure to prepare for the CMMC, but they are doing it without full understanding of the requirements. This all but guarantees millions of dollars of wasted effort when implementations are rejected as being insecure.

- Proposed Way Ahead

Assign a single office the authority and responsibility to respond to questions (and build an FAQ) about whether specific technical implementations or scope determinations are acceptable. Make these responses authoritative for CMMC assessments. Require this office to be responsive to C3PAO questions and public in their responses, to formulate new interpretive guidance for assessors and Organizations Seeking Certification (OSCs). Potential offices: DoD CIO, CMMC PMO

RECOMMENDATION

CMMC Project Management Office assign responsibility for technical clarification to a department within the DoD such as DoD CIO. The responsibility should include mandates for timely response (3 business days) to C3PAOs and certified assessors, public posting of question and answers, and authorization to apply the guidance to other companies facing the same situation.