POSITION PAPER SERIES

CMMC 2.0 L2 C3PAO Assessments

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 provide directional input from the C3PAO Stakeholder Forum to the DoD on which Defense Industrial Base (DIB) organizations should be required to be third party assessed. Provide a suggestion on how to get more third-party assessors ready and provide recommended criteria for the DIB that would be escalated over time.

DISCUSSION

It's critical that companies in the DoD supply chain get clarity on whether or not they will be needing to be third party assessed. Preparing for that type of assessment is a much heavier lift than a self-assessment. Rather than making these decisions on a contract-by-contract basis, we recommend a simpler, more predictable process that could be tightened over time.

DIB Issues

- DIB organizations have put the brakes on work to remediate their NIST POAMs.
- The DIB needs clarity in order to begin pressing hard now on getting compliant. Not knowing could impact their ability to be ready when required.
- PRIMES may over require small business to be third party assessed if the requirements are not clear to them.

C3PAO Issues

- The lack of clarity is already having a negative effect on the eco-system. C3PAOs are choosing not to seek certification. This is a time we need more authorized C3PAOs.
- At the current rate of DIBCAC C3PAO Assessments it will take double digit years to get everyone authorized.

Having clarity on who will need to be assessed will ensure market forces can be brought to bear on reducing the current high cost of solutions. A known market will reduce uncertainty and bring solution providers to the table. For example, the current high cost to subscribe to a Managed System Security Provider is prohibitive to a small business.

RECOMMENDATION

Assessments

We recommend using either a tailored set of National Security System (NSS) questions for DIB organizations or specific DoD CUI categories from NARA.

The tailored questions could come from NIST SP 800-59, Guideline for Identifying an Information System as a National Security System. Example questions:

- Does the information processed, stored or transmitted in the conduct of the contract involve intelligence activities?
- Does the information processed, stored or transmitted in the conduct of the contract involve cryptologic activities related to national security?
- Does the information processed, stored or transmitted in the conduct of the contract involve command and control of military forces?
- Does the information processed, stored or transmitted in the conduct of the contract involve equipment that is an integral part of a weapon or weapons system?
- Is the information processed, stored or transmitted in the conduct of the contract contribute to the direct fulfillment of military or intelligence missions?

Suggested CUI categories could be as follows:

- Controlled Technical Information
- DoD Critical Infrastructure Security Information
- Naval Nuclear Propulsion Information
- Unclassified Controlled Nuclear Information – Defense
- Export Controlled (DoD ITAR and DoC Controlled 600 Series)

Rather than making this based on a contract-by-contract basis, we recommend a simpler process that could be tightened over time. Possibly start with the NSS tailored questions, move to the DoD CUI categories, and then finally move to a broader set of CUI categories listed in the Supplementary Information.

For those DIB organizations not required to be C3PAO assessed, require them to submit substantiating documentation beyond a letter signed by an officer. Require them to submit their System Security Plan and Officer's Letter of Attestation to support their SPRS score. In addition, we recommend that they be required to provide the attestation of an individual who successfully completed the Certified CMMC Professionals (CCP) training, that their assessment was completed in accordance with the DoD CMMC Assessment Guidance.

C3PAOs

To increase the number of Level 2 assessments and thus reduce the overall risk to the DoD supply chain, we recommend allowing an interim approval process for authorizing C3PAOs. We recommend allowing them to submit their SSPs and evidence in order to give them an interim authority to assess until a DIBCAC assessment can be performed. This is a process like what is used by the Risk Management Framework as required by FISMA. The CMMC-AB could be used to review this documentation first before recommending the interim authorization to the DoD.

Increasing the number of Authorized C3PAOs is the first step. The second step is increasing the number of individuals authorized to participate on assessments. We recommend that assessment teams continue to require a Provisional Assessor (PA) to service as the Lead Assessor, until Certified CMMC Assessors (CCA) are available. We also recommend that individuals who have successfully completed Certified CMMC Professionals (CCP) training be allowed to participate on assessment teams, until the CCP

Exam is in place. This will greatly accelerate the number of teams C3PAOs can field to assess OSCs.

SUPPLEMENTARY INFORMATION

Critical Infrastructure

- Information Systems Vulnerability Information
- Physical Security
- Protected Critical Infrastructure Information

Defense

- Controlled Technical Information
- DoD Critical Infrastructure Security Information
- Naval Nuclear Propulsion Information
- Unclassified Controlled Nuclear Information - Defense

Export

- Export Controlled

Intelligence

- Operations Security

Nuclear

- Unclassified Controlled Nuclear Information – Energy

Privacy

- Military Personnel Records