POSITION PAPER SERIES

Gradually tighten cybersecurity expectations for contractors

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 encourage the Department of Defense to phase in CMMC compliance requirements gradually so that all CMMC ecosystem participants can gain experience and capabilities with less risk.

DISCUSSION

- Problem Statement

-- The majority of the Defense Industrial Base (DIB) is not meeting their contractual obligations for cybersecurity. This is not a minor deficiency. Most of the DIB does not even have a fully written system security plan. The average defense contractor would have difficulty meeting half of the CMMC Level 2 practices, let alone meeting all of them perfectly. The technical debt of the DIB is overwhelming.

-- Defense contractors lack institutional knowledge about cybersecurity compliance. Managed Service Providers and the typical DIB IT department has no experience with government-level expectations for cybersecurity. Their IT staff are not trained to understand cybersecurity controls. They have no idea of the level of effort required to prove compliance to an assessor.

-- The DoD's proposal to use time-limited Plans of Action & Milestones (POA&M) is flawed. If a company knows they have a deficiency but fails to fix it before their assessment, it is because there is no easy fix. Right now, defense contractors lack compliant solutions. Many have a functional need to use cloud services that lack proof of compliance. This is not a problem that will be fixed within 6 months of assessment.

-- If contractors cannot afford a single NOT-MET practice, they are more likely to escalate every finding for appeal. This raises the stakes of assessment for both the contractor and assessment team and distracts resources from the DoD and CMMC-AB that should be focused on clarifying expectations.

-- There are literally not enough cybersecurity compliance-trained personnel available to work with 80,000+ defense contractors to get them prepared for CMMC. This capability needs to be grown over time by preparing for assessment, getting assessed, fixing problems, and repeating. Gaining experience over time is key to building this workforce. Building sustainable demand is key to building this workforce.

-- Ironically, current CMMC assessors are suffering from a lack of work throughout all of this. Interest in "gap analysis" or "pre-assessments" is stagnant. To build the CMMC ecosystem, there needs to be demand. For demand to build, defense contractors need to know that CMMC will be enforced.

-- Provisional assessors and their C3PAOs need experience performing CMMC assessments. Defense contractors need to understand whether their scoping, proposed solutions, and evidence is acceptable. It would benefit both parties if assessments had room for variance during the first years of the CMMC program.

-- Right now, defense contractors seem to be taking the "you can't shoot us all" approach. They know that the DoD cannot enforce CMMC until most contractors have certificates or the threat of supply chain disruption will be too great. Defense contractors are watching the number of

certificates issued. They know that they have years and years before a critical mass is reached. Until that point, CMMC won't be enforced.

- Proposed Way Ahead

-- Before rulemaking is finalized, allow defense contractors to achieve CMMC certification with several NOT-MET practices.

-- Do not require any special authorization to be certified with NOT-MET practices. Do not require a POA&M or waiver. Instead, utilize a mathematical model such as the DoD Assessment Methodology to identify a minimum passing score. If the contractor exceeds that score, they receive CMMC certification.

-- Increase the minimum passing score each year until the desired compliance level is met. Defense contractors will be required to meet the higher score during their triennial re-assessment.

-- Identify very important security controls that must be MET to achieve CMMC certification. Keep this list as minimal as possible, focusing on risk-based governance activities rather than technology requirements, to provide flexibility to defense contractors.

-- Incentivize higher-than-minimum levels of compliance by considering the assessed compliance score during contract award.

-- By performing these steps, the following benefits will be achieved:

--- Defense contractors will increase their institutional knowledge of cybersecurity compliance over time.

--- The danger to the supply chain by enforcing CMMC against an unprepared DIB is reduced.

--- Defense contractors learn whether their solutions are acceptable years earlier, giving the contractors time to make major changes in order to reach 100% compliance.

--- Sustainable demand for assessors and cybersecurity staff, leading to increased numbers over time.

--- Defense contractors will start improving their cybersecurity stance incrementally rather than leaving the market upon enforcement or ignoring the requirement until it is too late.

--- Reduce appeals and complaints by defense contractors, freeing up DoD and CMMC-AB resources to assist the DIB in improving their cybersecurity stance.

--- Full cybersecurity requirements can be enforced on all defense contractors after the system is proven and a critical mass of contractors have certification. This achieves the original goal of CMMC while giving the ecosystem a needed opportunity to improve.

RECOMMENDATION

CMMC Project Management Office authorizes C3PAOs to award CMMC Level 2 certificates based on a minimum compliance score prior to rulemaking. Using a scoring approach similar to the DoD Assessment Methodology, the C3PAO Stakeholder Forum recommends starting with a minimum passing score of 60% immediately, increasing to 70% in the second year. After rulemaking, identify a new required compliance score, such as 90% or 100%, using knowledge gained during interim period.

SUPPLEMENTARY INFORMATION

Not Applicable