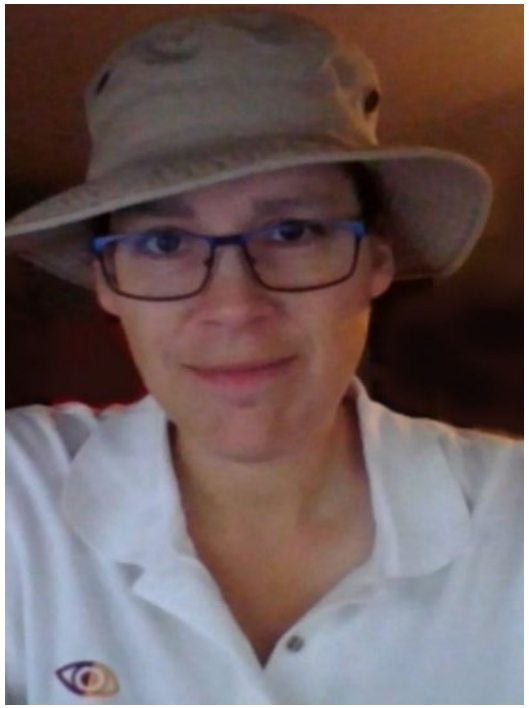
CMMC Update: Assessments

Current As Of: June 2024

Sponsored by:

TODAY'S SPEAKERS



Amira Armond

President
Kieri Solutions
Vice Chair, C3PAO Stakeholder Forum

Vince Scott

CEO
Defense Cybersecurity Group
INFRAGARD DIB Sector

Sponsored by:

2 Michael

Secure Your Networks and Systems In Physical Space and Cyberspace

- **Secure your Networks. Now**
- **Know your Contracts**
  - Your contracts should tell you what information you must protect
- **Define & Understand your business processes to identify how & where you store / handle / transmit CUI**

Sponsored by:

NDIA IT & Cybersecurity Survey - Preliminary

Sponsored by:

Definitions

- **Final Certification Assessment (CMMC Level 2)**
  - Performed and certified by a C3PAO
  - Requires perfect 110 score
  - Allows government to award contracts / sub-contracts / option years to company
  - Lasts for three years, can be renewed

Definitions

- **Conditional Certification Assessment (CMMC Level 2)**
  - Performed and certified by a C3PAO
  - Allows for some NOT-MET requirements
    - Scored 88 or better
    - No 5- or 3-point requirements missed
    - No level 1 requirements missed
  - Allows government to award contracts / sub-contracts to company
  - Lasts for 6 months. Cannot be renewed

Sponsored by:

Definitions

- **Self-Assessment (CMMC Level 2)**
  - Proposed rule uses term “Self-Assessment” to have similar meaning as “Certification Assessment” – this is confusing!
  - Performed by the company
  - Requires perfect 110 score
  - Allows government to award contracts / sub-contracts to company
  - Lasts for three years, with annual affirmations by company. Can be renewed

- **Conditional Self-Assessment (CMMC Level 2)**
  - Allows for some NOT-MET requirements
  - Allows government to award contracts / sub-contracts to company
  - Lasts for 6 months. Cannot be renewed

Assessment failure – what next?

- **Appeals**
  - Assessment team (primarily lead assessor) responsible for determining NOT-METs. C3PAO quality lead may overrule if they feel the decision was incorrect.
  - If appeal, an independent lead assessor for the same C3PAO will review *original evidence* and make their own call within 21 days.
  - If appeal denied, expect additional charge for assessor labor
  - Unlikely to be able to escalate past C3PAO. Cyber-AB's job to revoke accreditation of C3PAOs if they handle appeals poorly, not to handle escalations themselves.

Assessment failure – what next?

- **C3PAO required to enter result into eMASS reporting system**
  - Informed guess: Assessors will post results in CMMC eMASS (not yet available) & government employee will transfer to SPRS
  - Potential repercussions if have active DFARS 7012 contracts and/or a self-assessment recorded
- **Cannot be awarded contracts that require certification**
  - This includes option years
- **May be awarded contracts that require "self-assessment"**

Assessment failure – what next?

- **Allowed to get another assessment of just the NOT MET requirements?**
  - Not *disallowed* by the proposed rule
  - No guidance on allowable timeliness (6 months?)
  - No guidance if same C3PAO must perform, or if another C3PAO can leverage the audit report
  - An intrepid C3PAO may simply try it and see what happens
    - ***Current CMMC Assessment Process** (written by the Cyber-AB) does not really allow, however little to prevent it*

- **Contractor is allowed unlimited re-attempts, but cannot be awarded contracts that require certification during that time**

Sponsored by:

Assessment Fail: What next?

- **POA&M-acceptable topic**
  - Cannot use C3PAO as source of advice
  - Consider reaching out to a different assessor for advice on how to pass re-assessment

- **Must company use original assessor for re-assessment?**
  - No, but likely to be significantly less expensive because original assessor does not need to relearn the company

- **Failed because of a silly documentation issue?**
  - Seek C3PAOs that include a few hours of POA&M close-out assessment in the fixed price

Sponsored by:

Assessment Fail: What next? Impact

- **Existing Contracts**
  - Failure may not immediately impact existing contracts
  - DoD could establish program to alert in SPRS if <110 score entered
    - Could drive significant issues, especially if the failed company had key contracts
  - More likely: KO reviews SPRS score during annual contract review

- **New Contracts**
  - Failure drives ineligibility for new contracts
  - Companies part of teaming agreements for ongoing solicitations likely removed from team
  - KOs may remove/waiver certification requirement from new contracts if key bidders fail

Sponsored by:

Conditional certification – what next?

- **C3PAO required to enter result into eMASS reporting system**
  - Potential repercussions if have active DFARS 7012 contracts or a self-assessment recorded, but unlikely
- **May be awarded contracts that require certification**
  - This includes option years
- **May be awarded contracts that require "self-assessment"**
  - This includes option years

Sponsored by:

Conditional certification – what next?

- **Allowed to get another assessment of just the NOT MET requirements - YES**
  - Allowed multiple re-attempts of NOT-MET requirements within 180 days
  - No guidance in rule if same C3PAO must perform, or if another C3PAO can leverage the audit report.
    - CMMC Assessment Process (by Cyber-AB) explicitly allows other C3PAOs to do POA&M close-out.
  - If cannot achieve 110 score within 180 days, conditional certification expires
    - Standard contractual remedies apply
    - At this point it is too late to get a contract-wide waiver.

Sponsored by:

Assessment perfect score - what next?

- **Certificate issued by C3PAO**

- **Who will have access?**
  - Assessed company will receive copy of assessment report
  - Also receive a “certificate” to share with partners and/or future assessors
  - C3PAO who conducted assessment must confirm validity if requested
  - C3PAO will retain assessment report & certificate, but not “evidence”

Expectations after certification

- **DoD expects the certified information system will be used to store/process/transmit all CUI for the contract being awarded under the CAGE codes awarded per the contract**

- **Will contractors need to identify the system they plan to use in RFP responses?**
  - Dramatic additions to CUI scope (such as an acquisition) expected to be assessed out-of-cycle

- **Cannot abandon compliance efforts for duration of contract**

Sponsored by:

Expectations after certification

- **Schedule re-assessment with C3PAO in 32-34 months**

- **Maintain secure system operation**
  - This is NOT a fire and forget requirement
  - Continuous Monitoring required
  - Continuous action required (configuration management, change tickets, updating baselines, monitoring alerts etc etc etc)

- **Annual re-affirmation of 100% compliance**
  - This effectively mandates an annual self assessment
  - Affirmation = legal sworn oath of compliance from the “senior official” with corresponding personal federal fraud criminal liability

Long term

- **CMMC ecosystem evolves**
  - C3PAOs & implementers develop feedback loops
  - Likely leads to companies working with known / trusted entities
  - Ensures implementers understand what C3PAOs need to see
  - Ensures C3PAOs are predictable

- **Accreditation Body is tasked with preventing assessor fraud**
  - “Certification Mills”
  - Blatant conflicts of interest
  - C3PAOs punished by removing accreditation, invalidating certifications

Sponsored by:

Questions

Sponsored by: