DCMA

DEFENSE CONTRACT MANAGEMENT AGENCY

Candidate C3PAO Brown Bag

Presented By:

DIBCAC CMMC Assessment Team

Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)

April 15, 2021

Agenda

- Why We Are Here
- We Are NOT
- DIBCAC CMMC Assessment Team
- C3PAO Methodology
- Certification Assessment Readiness Review (CA-RR)
- Mechanics of the Assessment
- Post-Assessment
- DCMA Contact Information

Why We Are Here

- Office of the Under Secretary of Defense directed DCMA DIBCAC to validate compliance of Cybersecurity Maturity Model Certification (CMMC) Third-Party Assessor Organization (C3PAO) to the CMMC Level 3.

- We are verifying compliance using:
  - Cybersecurity Maturity Model Certification (CMMC), Version 1.02, March 18, 2020
  - CMMC Assessment Guide, Level 3, Version 1.10, November 30, 2020
  - CMMC Glossary and Acronyms2, Version 1.10, November 30, 2020
  - CMMC Appendices, Version 1.02, March 18, 2020
  - CMMC Errata, Version 1.10, November 30, 2020

Link: CMMC Model and Assessment Guides **https://www.acq.osd.mil/cmmc/draft.html**

We Are NOT

- Cybersecurity Maturity Model Certification (CMMC) Accreditation Body (AB)
- Submitting assessment results or reports to CMMC AB
- Conducting an **accreditation** or **certification** of enterprise or systems
- Conducting scans or penetration tests
- Providing recommendations
- Defending the wording in the CMMC Practices

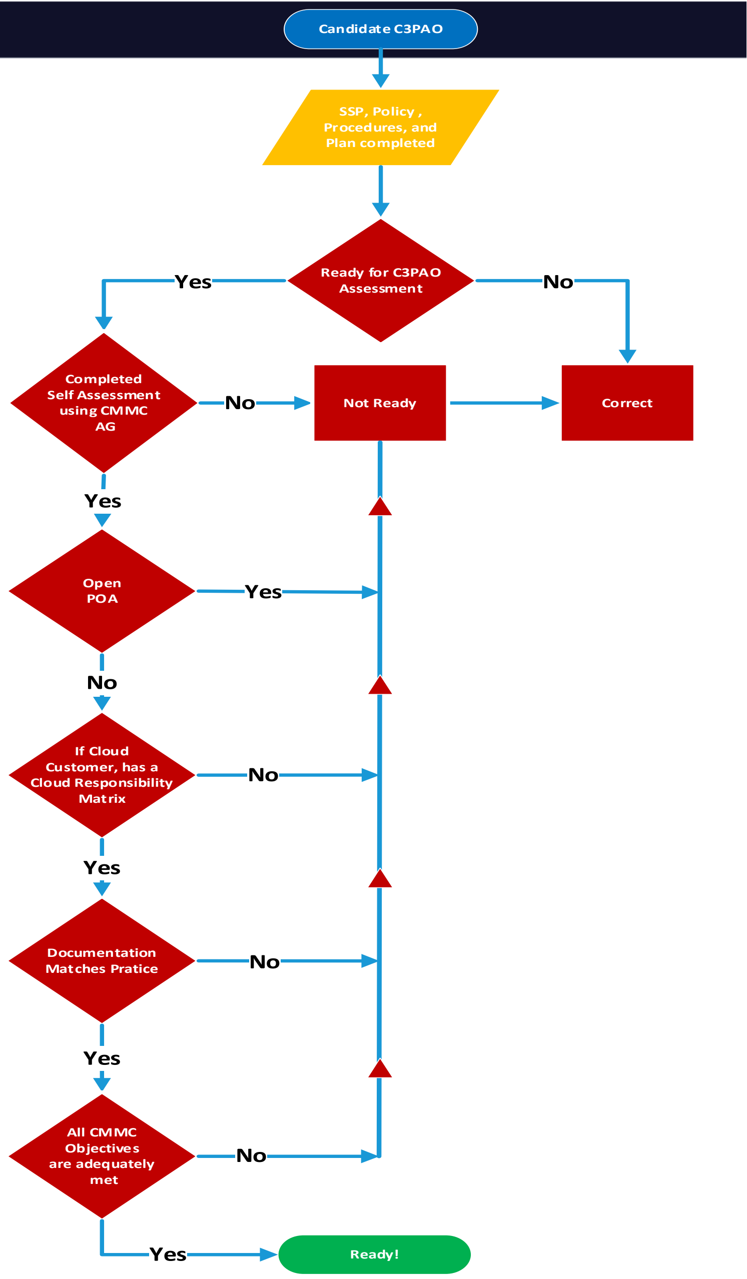
Training Slide

- DIBCAC Lead Assessors and Functional Lead Assessors are all trained and certified as per DoD Manual 8570.01-M, *Information Assurance Workforce Improvement Program*.
- As part of on-the-job training, all assessors have completed nine (9) Modules of classroom instruction, practical examinations, and hands-on assessments prior to assessing any Defense Industrial Base (DIB) company and all domain leads have attended training and received certification as a Certified Provisional Assessor via the CMMC Accreditation Body.
- Each DIBCAC CMMC assessor has completed at least five (5) DFARS clause 252.204-7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting,* assessments before participating in a CMMC assessment.

Links: DFARS clause 252.204-7012, https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting; DoD Manual 8570.01-M, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/857001m.pdf?ver=2019-07-08-101252-253

Are You Ready

- Documented SSP, Policy, Procedures, and Plan
- Completed Self Assessment with CMMC Assessors guide (signed by OSC leadership)
- No Open Plans of Action (POA)
- Added Cloud Customer Responsibilities Matrix actions to Procedures
- Procedures are repeatable and adequate to implement each practice
- All Practices objectives have been met
- Documents are not Draft



Candidate C3PAO

SSP, Policy , Procedures, and Plan completed

Ready for C3PAO Assessment

Yes

No

Correct

Completed Self Assessment using CMMC AG

No

Not Ready

Yes

Open POA

Yes

No

If Cloud Customer, has a Cloud Responsibility Matrix

No

Yes

Documentation Matches Pratice

No

Yes

All CMMC Objectives are adequately met

No

Yes

Ready!

Unclassified

Distribution A – Approved for Public Release, Distribution Unlimited

C3PAO Assessment Types

- **On-site**
  - Documentation will be provided in advanced
  - All assessors on-site
  - COVID and Budget dependent
- **Hybrid**
  - Documentation will be provided in advanced
  - One – Two (1 – 2) assessors on-site for validation of physical requirements
  - COVID dependent
  - Will use virtual collaboration tools and conference lines
- **Virtual**
  - Will use virtual collaboration tools and conference lines exclusively
  - Requires policy, procedures, and technical controls in place for meeting physical controls with alternate means
  - Cloud Service provided has to be responsible for physical practice

Unclassified
Distribution A – Approved for Public Release, Distribution Unlimited

Methodology

- During the CMMC assessment, the DIBCAC CMMC Assessor will verify and validate the Candidate C3PAO has properly implemented the practices and processes. Because a Candidate C3PAO can meet the assessment objectives in different ways (e.g., through documentation, computer configuration, network configuration, or training) **the DIBCAC CMMC Assessor may use a variety of techniques, including any of the three assessment methods described above from NIST SP 800-171A,** *Assessing Security Requirements for Controlled Unclassified Information,* **to determine if the contractor meets the intent of the practices and processes.**
- DIBCAC CMMC Assessor follows the guidance in NIST SP 800-171A when determining which assessment methods to use.
- DIBCAC CMMC Assessors are not expected to employ all assessment methods and objects contained within the assessment procedures identified in this publication. Rather, DIBCAC CMMC Assessors have the flexibility to determine the level of effort needed and the assurance required for an assessment (e.g., which assessment methods and assessment objects are deemed to be the most useful in obtaining the desired results). This determination is made based on how the Candidate C3PAO can accomplish the assessment objectives in the most cost-effective manner and with sufficient confidence to support the determination the CUI requirements are satisfied.
- Primary deliverable of an assessment is a report containing the findings associated with each practice and process. For more detailed information on assessment methods, see Appendix D of NIST SP 800-171A.
- DCMA DIBCAC CMMC Assessors also utilize the CMMC Assessment Guide Level 3, 20201208 and the CMMC Appendices V1.02, 20200318

Links: CMMC Model and Assessment Guides https://www.acq.osd.mil/cmmc/draft.html; NIST SP 800-171A https://csrc.nist.gov/publications/detail/sp/800-171a/final

DIBCAC CMMC Assessment Team

Assessment Lead

Deputy Assessment Lead

Assessment Team

Grouping 1

- Access Control (AC)
- Audit and Accountability (AU)
- Identification and Authentication (IA)

Grouping 2

- Awareness and Training (AT)
- Personnel Security (PS)
- Physical Protection (PE)
- Risk Assessment (RA)
- Security Assessment (CA)

Grouping 3

- Configuration Management (CM)
- Maintenance (MA)
- Media Protection (MP)
- Asset Management (AM)
- Recovery (RE)

Grouping 4

- Incident Response (IR)
- System & Communications Protection (SC)
- System & Information Integrity (SI)
- Situational Awareness (SA)

Unclassified

Distribution A – Approved for Public Release, Distribution Unlimited

DIBCAC Leadership, Oversight, and Observers

DIBCAC Director

DIBCAC CMMC Oversight

Leadership and Oversight Roles: To obtain information / knowledge to improve the assessment program.

Assessment Team Observers (Right-Seat-Riders (RSR))

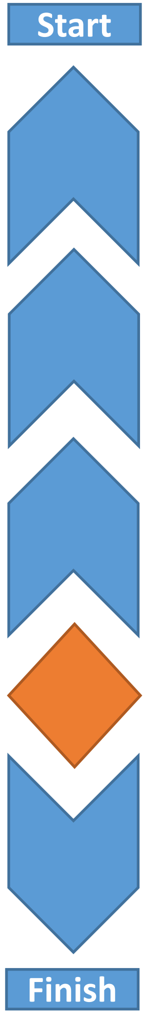
RSR purpose is strictly limited to "observation" in order to acquire a better understanding of the DIBCAC CMMC assessment process to obtain information / knowledge to improve DIBCAC's processes and procedures.

These attendees are not involved in the assessment, nor do they interact with Candidate C3PAO personnel during the week of the assessment.

Unclassified
Distribution A – Approved for Public Release, Distribution Unlimited

Assessment Timeline

DIBCAC CMMC Assessors utilize the CMMC Level 3 Assessment Guide, and CMMC Appendices to assess Candidate C3PAOs on the following 6 – Week schedule:


Start

Finish

- 4 Weeks Prior to Assessment - Pre-coordination Meeting

  (Meet DIBCAC CMMC Lead Assessor and Candidate C3PAO POCs, Request DoD Secure Access File Exchange (SAFE) Drop of System Security Plan (SSP), Policy Procedures, Customer Responsibility Matrix, and Documentation Traceability Matrix)

- 2 Weeks Prior to Assessment - Receive SSP, Policy, and Procedures
  - Review Documentation for Readiness Review (Internal)
  - Readiness Review with Candidate C3PAO – **Go/No Go** (End of week)
  - Self-Assessment Results signed by Chief Information Security Officer (CISO) or Chief Information Officer (CIO)
- 1 Week Prior to Assessment
  - Finalize Assessment Plan
  - Finalize Interview and Demonstration schedule

- **Assessment Week**

  Execute
- 1 – 2 Weeks Post-Assessment
  - Assessment Buffer (2 days)
  - Finalize notes, report, and memorandum
  - Final Memorandum with report to OUSD within 10 business days of Out-brief

Certification Assessment Readiness Review (CA-RR)

- **Determination to proceed with Candidate C3PAO**
  - Go = Documentation demonstrates candidate is CMMC Level 3 ready, assessment proceeds
  - Stop = Documentation does not meet CMMC Level 2 Practices, assessment stops

  <u>CMMC Level 1 only possible outcome of Assessment</u>
- **SSP**
  - Still in a draft
  - Template was not completed (i.e. Insert Text Here)
  - Mismatches with Policy
  - Mismatches with Inheritance
- **Policy**
  - Still in a draft
  - Templates not completed
  - Mismatches with SSP
- **Procedures**
  - Still in a draft
  - Templates not completed (i.e. Insert Text Here)
  - Distinguishing between policy and procedures Not clear
  - Could not determine who to interview
  - Could not determine what to test
- **Plans of Action (POA)**
  - Open POA
- **Scoping**
  - Only C3PAO environment will be in scope

Unclassified

Distribution A – Approved for Public Release, Distribution Unlimited

CA-RR Concerns

Concerns:

- No Cloud Service Provider “Customer Responsibility Matrix” provided
  Inheritance matrix not clearly related to SSP, policy, and procedures

- SSP identifies, but no procedures referenced for these Cloud systems

- User End points / Bring Your Own Device (BYOD)
  - Identified in Diagram
  - SSP and Policy verbiage does not align
  - Policy / technical controls associated with these systems not clear

Unclassified

Distribution A – Approved for Public Release, Distribution Unlimited

Interview

Who Is Interviewed:

- The DIBCAC CMMC Assessor has discussions with individuals within an organization to understand if a practice or process has been addressed. **Interviews of applicable staff** (possibly at different organizational levels) determine if CMMC practices or processes are implemented as well as if adequate resourcing, training, and planning have occurred for individuals to perform the practices.

- Important! Who is interviewed is determined based off documentation (policy and procedures).

Examined

What Is Examined:

- Examination includes reviewing, inspecting, observing, studying, or analyzing assessment objects. The objects can be documents, mechanisms, or activities.
- For some practices or processes, the DIBCAC CMMC Assessor reviews documentation to determine if assessment objectives are met. Interviews with contractor staff may identify the documents the contractor uses. Documents need to be in their final forms; working papers (e.g., drafts) of documentation are not eligible to be submitted as evidence because they are not yet official and are still subject to change. Common types of documents usable as evidence include:
    - policy, process, and procedure documents;
    - training materials;
    - plans and planning documents; and
    - system-level, network, and data flow diagrams.
- This list of documents is not exhaustive or prescriptive. A contractor may not have these specific documents, and other documents may be used to provide evidence of compliance.
- In other cases, the practice or process is best assessed by observing that safeguards are in place by viewing hardware or associated configuration information or observing staff following a process.

Tested

What Is Tested:

- Testing is an important part of the assessment process. Interviews tell the DIBCAC CMMC Assessor what the Candidate C3PAO staff believe to be true, documentation provides evidence of intent, and testing demonstrates what has or has not been done.
- For example, Candidate C3PAO staff member may **talk about how users are identified**; **documentation may provide details on how users are identified**, but **seeing a demonstration of identifying users provides evidence the practice is met.**
- **The DIBCAC CMMC Assessor will determine which practices or objectives within a practice, need demonstration or testing.** Not all practices will require testing.

- Important! What is Tested is determined based off documentation (policy and procedures).

Assessment Results

- The assessment of a CMMC practice or process results in one of three possible findings: MET, NOT MET, or NOT APPLICABLE. To achieve a specific CMMC level, the contractor will need a finding of MET or NOT APPLICABLE finding on all CMMC practices and processes required for the desired level as well as for all lower levels. For example, a contractor will need a MET or NOT APPLICABLE finding on all CMMC practices and processes at Levels 3, 2, and 1 **to achieve a CMMC Level 3 certification**.

- **MET:** The C3PAO Candidate successfully meets the practice or process. For each practice or process marked MET, the Certified Assessor includes statements that indicate the response conforms to the objectives and documents the appropriate evidence to support the response.

- **NOT MET:** The C3PAO Candidate has not met the practice or process. For each practice or process marked NOT MET, the Certified Assessor includes statements that explain why and documents the appropriate evidence that the contractor does not conform to the objectives.

Assessment Results

- **NOT APPLICABLE (N/A):** The practice or process does not apply for the assessment. For each practice or process marked N/A, the Certified Assessor includes a statement that explains why the practice or process does not apply to the Candidate C3PAO. For example, Systems and Communications Protection (SC).1.176 might be not applicable (N/A) if there are no publicly accessible systems.
- A Candidate C3PAO can **inherit** practice or process objectives. A practice or process objective that is inherited is met because adequate evidence is provided that the enterprise or another entity, such as an External Service Provider (ESP), performs the practice or process objective.
- **Evidence from the enterprise or the entity from which the objectives are inherited should show they are applicable to in-scope assets and that the assessment objectives are met.** For each practice or process objective that is inherited, the Candidate C3PAO includes statements that indicate how they were evaluated and from whom they are inherited. **If the Candidate C3PAO cannot demonstrate adequate evidence for all assessment objectives, through either Candidate C3PAO evidence or evidence of inheritance, the Candidate C3PAO will receive a NOT MET for the practice or process.**

Post-Assessment

Official Results reported to OUSD (within 10 business days)

- Notes (Assessment scoring method sheet)
- Report
- Out-brief
- Memorandum

Remediation

- Assessment Remediation may be required if the Candidate C3PAO comes close to meeting their Level goal, but fall short on a few practices. There is an opportunity to perform a "remediation assessment" on the missed practices within 90 days of Out-brief.
- If the Candidate C3PAO does not pass the majority of a level, a "remediation" appraisal will not be granted.
- Remediation assessment ("delta assessment") must be completed within 90 days of remediation request and practices must demonstrate persistent use.
- DIBCAC Governance Board reviews the request (from Candidate C3PAO) to 'approve or deny' to proceed with "delta assessment".
- If approved, the Assessment Lead/team will review requested practice areas to include updated objective evidence, verify and determine if met/ not met, and report results to OUSD within 10 business days of "delta assessment" completion.

Adjudication Governance

- **The Candidate C3PAO shall have the opportunity to dispute assessment results within seven (7) business days of Out-brief to the Lead Assessor.**

  (*Reminder:* Final report is due to OUSD with 10 business days of Out-brief.)

- **Lead Assessor receives Adjudication request from the Candidate C3PAO**
- **DIBCAC Governance Board:**
  - **Reviews –**
    - **Request**
    - **Objective evidence provided during the assessment**
    - **Notes and artifacts pertaining to adjudication item(s) requested**
    - **Comments from Candidate C3PAO,**
  - **Makes Determination – Change Assessment or Not**
- **Reserves the right to talk with:**
  - **National Institute of Standards and Technology (NIST)**
  - **DoD Chief Information Officer (CIO)**
  - **CMMC Program Management Office (PMO)**
- **Determination provided to Lead Assessor and final report can be completed with final determination**
- **All adjudication actions shall be completed and/or resolved within 20 business days**

DCMA Contact Information

DIBCAC POC: dcma.lee.hq.mbx.dibcac-cmmc@mail.mil

Questions

Acronyms

Acronym	Description
&	and
AB	Accreditation Body
BYOD	Bring Your Own Device
C3PAO	Certified Third Party Assessor Organization
CA-RR	Certification Assessment Readiness Review
CIO	Chief Information Office
CMMC	Cybersecurity Maturity Model Certification
COVID	Severe acute respiratory syndrome coronavirus 2, SARS-CoV-2, previously known by the provisional name 2019 novel coronavirus, 2019-nCoV
DCMA	Defense Contract Management Agency
DIB	Defense Industrial Base
DIBCAC	Defense Industrial Base Cybersecurity Assessment Center
DoD	Department of Defense
DFARS	Defense Federal Acquisition Regulation Supplement

Acronym	Description
e.g.	For Example
eMASS	Enterprise Mission Assurance Support Service
ESP	External Service Provider
ISO	International Organization for Standardization
N/A	Not Applicable
NIST	National Institute of Standards and Technology
OUSD	Office of the Undersecretary of Defense
PMO	Program Management Office
POA	Plans of Action
POC	Point of Contact
SAFE	Secure Access File Exchange
SC	Systems and Communications Protection
SP	Special Publication
SSP	System Security Plan

Unclassified
Distribution A – Approved for Public Release, Distribution Unlimited

Useful Links

- CMMC Model and Assessment Guides: https://www.acq.osd.mil/cmmc/draft.html
- Cybersecurity Frequently Asked Questions: https://dodprocurementtoolbox.com/faqs/cybersecurity
- DFARS Part 252: https://www.acquisition.gov/dfars/part-252-solicitation-provisions-and-contract-clauses
- NIST SP 800-53R5: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- NIST SP 800-171A: https://csrc.nist.gov/publications/detail/sp/800-171a/final
- NIST SP 800-171R2: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
- NIST SP 800-172: https://csrc.nist.gov/publications/detail/sp/800-172/final NIST Computer Security Resource Center (CSRC) https://csrc.nist.gov/publications/sp800
- Office of the Under Secretary of Defense for Acquisition & Sustainment Cybersecurity Maturity Model Certification: https://www.acq.osd.mil/cmmc/index.html