## Purpose: The purpose of this document is to provide the candidate Cybersecurity Maturity Model Certification Third Party Assessment Organization (C3PAO) (hereafter referred to as candidate) planning guidance and a notional schedule for a CMMC Level 2 assessment in accordance with the CMMC Assessment Guide – Level 2[[1]](#footnote-2). The CMMC Assessment Guide – Level 2 is the primary and authoritative source of guidance for the candidate C3PAO assessment. This guide is based upon the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171A, “Assessing Security Requirements for Controlled Unclassified Information.” The CMMC Assessment Guide – Level 2 also addresses CMMC prerequisites for assessment scoping. These prerequisites are addressed in detail in the CMMC Assessment Scope – Level 2.

**Pre-assessment planning activities:**

1. The candidate acknowledges receipt of assessment notification sent via email (within five business days).
2. The candidate downloads a blank copy of the Pre-Assessment Package from the DCMA DIBCAC website (https://www.dcma.mil/DIBCAC).

|  |
| --- |
| **Guidance:**  Documents included in the package are:   1. **TAB A** – *Controlled Unclassified Information (CUI) Handling Agreement*. The candidate’s representative is responsible for managing the consent record for all  non-federal personnel participating in any meeting with DIBCAC staff. If the candidate needs to modify this document prior to the assessment, an updated version can be provided to the DIBCAC Assessment Lead. 2. **TAB B** – *Candidate C3PAO Intake Form TAB B* requires details on the candidate’s organization and the intended C3PAO environment. 3. **TAB C** – *Candidate C3PAO "INHERITED/PARTIALLY INHERITED/NOT APPLICABLE REQUIREMENTS"* requires candidate to designate requirements that are inherited, partially inherited or not applicable (if any). 4. **TAB D** – *Candidate C3PAO "ASSET INVENTORY"* requires candidate to describe the organization’s asset inventory in order to define the assessment scope. This is in accordance with the CMMC Assessment Guide – Level 2, Assessment Scope requirement (reference pages 3 – 4), “Prior to conducting a CMMC assessment, the contractor must specify the CMMC Assessment Scope. The CMMC Assessment Scope informs which assets within the contractor’s environment will be assessed and the details of the assessment. To specify the CMMC Assessment Scope, contractors will map their assets into one of the following five categories: CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, and Out-of-Scope Assets....” Use of the template is optional; however, all asset categorization requirements should be addressed in the inventory artifact provided to DIBCAC.  A corporate inventory format may be used as long as the asset types support the CMMC Model 2.0 framework requirements. 5. **TAB E** – *Visitor Information Worksheet* addresses visitor requirements for the  on-site component of an assessment (if needed). *[The Assessment Lead will determine if there will be an on-site component after the scoping call is conducted.]* |

1. The candidate gathers scoping artifacts to send to DIBCAC.

|  |
| --- |
| **Guidance:**  In addition to the notification package, there are other artifacts that should be provided to DIBCAC prior to the scoping call. CMMC Assessment, Level 2 – Pre-assessment Planning and Scoping items represent the candidate’s compliance with the CMMC Assessment  Scope – Level 2 requirement (reference page 3), “The contractor [candidate C3PAO] is required to document all asset categories that are part of the assessment scope in an asset inventory and provide a network diagram of the assessment scope to facilitate scoping discussions during pre-assessment activities.” Other pre-assessment artifacts include topology diagrams with asset mapping; data flow diagrams; System Security Plan (SSP); and customer responsibility matrix, or equivalent, for inherited requirements. |

1. The candidate requests a DoD SAFE drop link from the DIBCAC Assessment Lead.
2. The DIBCAC Assessment Lead sends a DoD SAFE drop link to the candidate.
3. The candidate sends the pre-assessment package documents and scoping artifacts to DIBCAC via DoD SAFE (no later than two weeks prior to scoping call).

|  |
| --- |
| **Guidance:**  DIBCAC uses DoD SAFE to support encrypted artifact transfers. Link is <https://safe.apps.mil/about.php>.  (See images after instructions below for reference.)   * 1. Copy the link from the email sent by DIBCAC and complete the drop request:  1. To:  Assessment Lead / Assessors 2. Check:  “Encrypt every file” (Required) 3. Click or drag files to upload 4. Add short note to the recipients 5. Name:  CMMC C3PAO Assessments – Requirement, objective, company name,  date (i.e., AC.L1-3.1.1 \_a\_XX-C3PAO-XXXX\_CompanyName\_20220325) 6. Note:  Requested Materials Attached.  Sender’s Name 7. If uploading many documents, group in folders under family (i.e. AC.L1-3.1, 3.2, etc.) and zip entire folder structure into a single file for ease of uploading and downloading     1. To add multiple recipients at once: 8. Select “Add Many” 9. List names and email addresses (include designated DIBCAC Assessment Lead) 10. Click “Add & Close” to proceed      1. To add files: 11. Click the “Click to Add Files or Drag Them Here” 12. Select files or just drag them to the screen      1. To encrypt files: 13. Check the “Encrypt every file” box 14. Enter passphrase 15. Enter passphrase again (must be at least 10 characters) 16. Provide passphrase to DIBCAC Assessment Lead via alternate methods (email or phone call)   *Figure 1- Example - DoD SAFE Drop Request*  *Figure 2- Example - DoD SAFE*  *Please refer to Section 3 in the DoD SAFE User Guide for additional file drop-off information (https://safe.apps.mil/help/dod-safe-help.xml).* |

1. The candidate and DIBCAC hold a scoping call (approximately eight weeks prior to assessment start).

|  |
| --- |
| **Guidance:**   * The scoping call will be scheduled by the DIBCAC Assessment Lead who will provide an invite to the candidate. * DIBCAC uses the Department of Defense (DoD) instance of Microsoft (MS) Teams as the primary assessment collaboration tool.   + To minimize latency issues, DIBCAC also recommends not using video for MS Teams meetings.   + Please note you cannot access the DoD instance of MS Teams from the commercial version of the MS Teams application. You will need to access MS Teams using the web browser. The following information may assist with access:     1. Open Google Chrome or MS Edge.     2. Clear your selected browser’s cache. Recommend for the time range you select ‘All Time.’     3. Return to the meeting invitation in either MS Outlook or in your MS Teams calendar.     4. Copy and paste the DoD MS Teams URL into the address bar of your browser (Google Chrome or MS Edge).     5. Click ‘Cancel’ when prompted to open the MS Teams application and select ‘Watch on the Web.’ * Prior to the scoping call (days before or just prior to the call beginning), the Assessment Lead may elect to hold a communications check. * The DIBCAC Assessment Lead will discuss the items received from the candidate  (pre-assessment package and scoping artifacts) in order to define the assessment scope. * Optional – consider sharing the portions of your System Security Plan demonstrating the assets are present as required by the CMMC Assessment Scope – Level 2 guide’s detailed descriptions for each asset category. * If the candidate is determined “not ready” for an assessment based on the scoping call, the Cyber Accreditation Body (AB) will be notified of the status and the candidate’s status will be sent back to the Cyber AB. |

1. Based on the outcome of the scoping call, DIBCAC will determine whether the assessment will be a hybrid (virtual and on-site component) or virtual-only, and will share that decision with the candidate.
2. The period between the scoping call and assessment start is available for detailed assessment plan coordination activities between the candidate representative and the DIBCAC Assessment Lead.
3. The candidate gathers final version of the System Security Plan(s) (SSPs) and all referenced artifacts to send to the DIBCAC Assessment Lead (no later than two weeks prior to assessment start).

|  |
| --- |
| **Guidance:**  Artifacts needed in advance of the assessment start include and may not (depending upon the environment) be limited to the items listed below.   * The SSP(s) must clearly address how each of the 110 requirements found in the CMMC Assessment Guide – Level 2 are implemented at the objective level within your candidate C3PAO environment, and demonstrate your C3PAO organization correctly understands each of the requirements. CA.L2-3.12.4 addresses elements for a good SSP, which often include, but are not limited to: * General system description * Description of system boundaries * System environments of operation   + Major applications   + General support systems   + Minor applications   + Information System(s) relationships with/or connections to other systems (internal and external)   *Note that simply copying/pasting the requirement/objective verbiage from the CMMC Assessment Guide – Level 2, and/or the NIST SP 800-171A without a description of how it is implemented would not be acceptable.*   * As the CMMC Level 2 assessment is conducted at the requirement **objective** level, the CMMC Assessment Guide – Level 2 suggests the supporting artifacts describe how each objective is implemented to include: * Reference to a policy or technology/tool should include an explanation of how it ties directly to the requirements * All supporting documentation referenced in the SSP should be made available to the Assessment Team * Provide artifacts for inherited requirements that are considered ‘Met’ by a document such as a policy, process, or log, to include highlighting the specific section of the policy/process that applies to the specific ‘Met’ requirements * Describe how the organization will use and protect Organization Seeking Certification (OSC) artifact files and proprietary data used as objective evidence in an assessment to include maintaining file integrity as it existed when reviewed by an assessor; the storage of the file/artifact on the OSC network; and if part or all of this information is retrieved post-assessment, how would any file/artifact modification be evident * Artifact revision history * A detailed Network Topology Diagram/Network Enterprise Overview Briefing (to include a high-level operational concept graphic, or OV-1), and diagram of the candidate’s intended C3PAO environment’s network for handling, transmitting, and storing CUI, to aid in the DIBCAC’s understanding of how your requirement implementations are protecting CUI. This diagram must depict the network topology and security posture of the information systems or network processing CUI data. The drawing/overview briefing must clearly delineate (as applicable):   + Security boundaries   + Cybersecurity stack   + Security event information management   + Connections to other systems/networks   + Cloud interconnections/data flow   + Wireless (Institute of Electrical and Electronics Engineers (IEEE) standard 802.11)   + Dedicated point-to-point connections   + Multi-Protocol Label Switching (MPLS) clouds   + High-level Internet Protocol (IP) address schema   + Critical network enterprise services   + Vulnerability scanning methodology   + Authentication methodology   + Enterprise logging   + Remote access   + VoIP (Voice over Internet Protocol)   + Video   + Any other relevant information to allow the assessors to determine if your C3PAO environment is protecting CUI, as required by the 110 requirements and their objectives.   Suggest reviewing the CMMC Assessment Guide – Level 2 to read the discussion and further discussion sections addressing each requirement to enhance an understanding of the depth and rigor of the CMMC Level 2 assessment at the requirement objectives level. |

1. The candidate requests a DoD SAFE drop link from the DIBCAC Assessment Lead.
2. The DIBCAC Assessment Lead sends a DoD SAFE drop link to the candidate.
3. The candidate sends the pre-assessment package documents and scoping artifacts to DIBCAC via DoD SAFE (no later than two weeks prior to scoping call).
4. DIBCAC and candidate will develop and agree to an Assessment Plan before the assessment start date (no later than three days prior to the start of the assessment).

**Assessment activities:**

DIBCAC conducts the assessment.

|  |
| --- |
| **Guidance:**  During the assessment, DIBCAC will conduct interviews and review appropriate evidence and/or demonstrations in order to determine if the requirements are ‘met.’ DIBCAC requests access to the following:   * + Members of the policy team tasked with maintaining policies, which ensure cybersecurity compliance with the 110 requirements at the objective level addressed in the CMMC Assessment Guide – Level 2.   + Internal audit members tasked with responsibilities in cybersecurity.   + Internal audit records showing governance associated with cybersecurity.   + Subject Matter Experts (SMEs) by role and or position who can demonstrate implementation and answer questions. The SMEs should be available for each requirement interviewed. Examples of positions/personnel include:     - * Network Administrator/Engineer       * Employees with audit and accountability responsibilities       * Employees with cybersecurity/Information Technology (IT) policy oversight       * Account Management personnel       * Personnel with information security responsibilities       * System Developers       * Personnel with access enforcement responsibilities       * Risk Assessment Team       * Cyber Net Defender/Incident Response       * Senior Information Security Officer       * Training/Personnel/Human Resources Specialist       * Physical Security Specialist       * Employees with configuration management responsibilities       * Enterprise Services Lead       * Active Directory Administrator |

**Additional Items:**

**DCMA DIBCAC CMMC Level 2 (L2) Requirement Family Groups**

*[Red underline indicates that assessors may need to be physically present to assess these requirements.]*

|  |
| --- |
| Group 1: 42 Requirements |
| AC.L1-3.1.1/2/20/22  AC.L2-3.1.3/4/5/6/7/8/9/10/11/12/13/14/15/16/17/18/19/21  AU.L2-3.3.1/2/3/4/5/6/7/8/9  IA.L1-3.5.1/2  IA.L2-3.5.3/4/5/6/7/8/9/10/11 |
| Group 2: 18 Requirements |
| AT.L2-3.2.1/2/3  PS.L2-3.9.1/2  PE.L1-3.10.1/3/4/5  PE.L2-3.10.2/6  RA.L2-3.11.1/2/3  CA.L2-3.12.1/2/3/4 |
| Group 3: 24 Requirements |
| CM.L2-3.4.1/2/3/4/5/6/7/8/9  MA.L2-3.7.1/2/3/4/5/6  MP.L1-3.8.3  MP.L2-3.8.1/2/4/5/6/7/8/9 |
| Group 4: 26 Requirements |
| IR.L2-3.6.1/2/3  SC.L1-3.13.1/5  SC.L2-3.13.2/3/4/6/7/8/9/10/11/12/13/14/15/16  SI.L1-3.14.1/2/4/5  SI.L2-3.14.3/6/7 |

**Notional Assessment Schedule (One Room Model)**

*All times are planned for the candidate’s mailing address time zone.*

Day One 0830 – 1000 DIBCAC/Candidate In-Briefs

1000 – 1200 System Security Plan and Additional Documentation Review

1200 – 1300 Lunch

1300 – 1600 System Security Plan and Additional Documentation Review

1600 – 1630 Afternoon Artifact Request

Day Two 0815 – 0830 Arrival (on-site as applicable) and Connectivity Tests/Troubleshooting (virtual)

0830 – 1200 Group1 Requirements:

AC – 3.1

AU – 3.3

IA – 3.5

1200 – 1205 Morning Artifact Request

1200 – 1300 Lunch

1300 – 1530 Group 3 Requirements:

CM – 3.4

MA – 3.7

MP – 3.8

1530 – 1600 DCMA Internal Discussion

1600 – 1630 Afternoon Artifact Request and Daily Checkpoint (daily summary)

Day Three 0800 – 0830 Arrival (on-site as applicable) and Connectivity Tests/Troubleshooting (virtual)

0830 – 1200 Group 2 Requirements:

AT – 3.2

PS – 3.9

PE – 3.10

RA – 3.11

CA – 3.12

1200 – 1205 Morning Artifact Request

1200 – 1300 Lunch

1300 – 1530 Group 4 Requirements:

IR – 3.6

SC – 3.13

SI – 3.14

1530 – 1600 DCMA Internal Discussion

1600 – 1630 Final Artifact Request and Daily Checkpoint (daily summary)

Day Four 0800 – 0830 Arrival (on-site as applicable) and Connectivity Tests/Troubleshooting (virtual)

0830 – 1200 Requirement Follow-ups, as required

1200 – 1205 Final Artifact Delivery Deadline (if required)

1200 – 1300 Lunch

1300 – 1530 Requirement Follow-ups, as required

1530 – 1600 DCMA Internal Discussion and/or Out-Brief Prep

1600 – 1630 DCMA Out-Brief and Discussion   
(Daily Checkpoint if assessment not complete)

Day Five 0800 – 0830 Arrival (on-site as applicable) and Connectivity Tests/Troubleshooting (virtual)

TBD(If assessment is not complete) Requirement   
Follow-ups, as required

TBD DCMA Out-Brief and Discussion

1. <https://dodcio.defense.gov/CMMC/Documentation/> November 16, 2022 [↑](#footnote-ref-2)