

CONTROLLED//PROPIN When Filled In
Candidate CMMC Third Party Assessment Organization (C3PAO)
Intake Form - TAB B

Purpose: The candidate Cybersecurity Maturity Model Certification (CMMC) Third Party Assessment Organization (C3PAO) [hereafter referred to as “candidate”] is requested to:

1. Complete the CMMC Level 2 assessment intake form.
2. Return the completed form to DCMA DIBCAC as part of the pre-assessment planning and scoping artifact package provided in support of a CMMC Level 2 assessment.

Controlled by: Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) DCMA-TDX

CUI Category: General Proprietary Business Information

Distribution/Dissemination Control: Dissemination List
Controlled

POC: DCMA DIBCAC-CMMC, dcma_dibcac_cmmc@mail.mil

CONTROLLED//PROPIN When Filled In
Candidate CMMC Third Party Assessment Organization (C3PAO)
Intake Form - TAB B

Dissemination List Controlled – Do Not Separate from Intake Form

Dissemination of the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) Candidate CMMC Third Party Assessment Organization (C3PAO) Intake Form for _____ is limited to:

1. Employees of the United States (U.S.) Government executive branch agencies or Military Services personnel.
2. _____ and the _____ and the following corporate employees authorized access by:

CONTROLLED//PROPIN When Filled In
Candidate CMMC Third Party Assessment Organization (C3PAO)
Intake Form - TAB B

SECTION I: BASIC CANDIDATE C3PAO INFORMATION

1. Organization Name:
2. Physical Address:
3. Lead Candidate Representative Name/Title:
4. Assessment POC Name/Title (if different from above):
5. Host Unit (if applicable):
6. Supporting Unit(s) (if applicable):
7. Unique Entity Identifier (UEI):
8. Primary Assessment Location:
9. Briefly describe the organization's mission in the box below.

CONTROLLED//PROPIN When Filled In
Candidate CMMC Third Party Assessment Organization (C3PAO)
Intake Form - TAB B

Basic Candidate C3PAO Information (Continued)

10. Does the candidate's organization support any active Department of Defense contracts?
11. Within the past 12 months, has the organization participated in any merger or acquisition?
(If yes, please state with whom and when.)
12. Does the organization plan to participate in a merger or acquisition within the next 12 months?
(If yes, please state with whom and when.)
13. Is the candidate C3PAO initiative organizationally a separate company or a division?
14. What is the name of the separate company or division the C3PAO environment is aligned under?
15. Describe the C3PAO environment location (physical and/or virtual).
16. List all past and present office locations (City, State, and Country).
17. Are all the office locations listed on the same network and do they have the same protections as the rest of the organization performing C3PAO duties?
18. Where are the assessors located when not working on-site at an Organization Seeking Certification (OSC) (City, State, and Country)?
19. Explain conditions for staff at locations outside of the United States and its territories that would have access to the C3PAO environment (if applicable).

CONTROLLED//PROPIN When Filled In
Candidate CMMC Third Party Assessment Organization (C3PAO)
Intake Form - TAB B

SECTION II: SCOPING INFORMATION

Endpoints

- 20. Will the assessors use organization-controlled computing devices to include mobile phones, tablets, laptops, and/or desktops?
- 21. Does the organization permit assessors to use their own devices?
[Bring Your Own Device (BYOD)]
- 22. Does the environment utilize a virtual desktop infrastructure tool?

Physical Security

- 23. Does the organization centrally manage the physical security at all of the locations supporting the C3PAO environment?
- 24. Does the C3PAO environment have a physical footprint such as servers, printers, and/or multi-function devices besides the endpoints?

System Security Plan

- 25. Is the C3PAO environment addressed in an enterprise or enclave System Security Plan (SSP)?
- 26. For inherited practices does the C3PAO environment's SSP reference the other SSP from which the inherited practice is derived?
- 27. Does the C3PAO environment's SSP include the relationship(s) with or connection(s) to other asset(s) listed in the asset inventory?
- 28. Does the C3PAO environment's SSP identify how security requirements are implemented for specialized assets not physically or logically separated from CUI assets?

Incidents/Events/Reporting

- 29. Briefly describe the organization's experience with incident reporting.
- 30. Briefly describe any organizational experience(s) with cyber events occurring in the past 12 months.
- 31. Summarize how the organization interacts with any external service providers in support of the incident and event management processes (if applicable).

CONTROLLED//PROPIN When Filled In
Candidate CMMC Third Party Assessment Organization (C3PAO)
Intake Form - TAB B

Incidents/Events/Reporting (Continued)

32. Does the organization's event management process support the retention and maintenance of detailed records of events for analysis?

Information Systems

33. Describe the model for ensuring objective evidence/artifacts from C3PAO assessments will remain unmodified when stored in the OSC environment.
34. Describe the organization's approach to aggregating and reviewing information system log data.
35. Describe any backup services used by the organization to support the C3PAO environment.

External Service Provider

36. Does the C3PAO environment use an External Service Provider (ESP) for? (check all that apply)
- | | | |
|---|------------------------------|---------------------|
| Cloud Service Provider (CSP) | Security Protection Services | Customized Software |
| Hosted Virtual Private Network (VPN) services | Managed Service Provider | |
37. If using a CSP, are they authorized as FedRAMP Moderate?
38. If using a CSP that is not authorized as FedRAMP Moderate, does the CSP? (check all that apply)
- | | | | |
|-----------|-------------|--------------|----------------|
| Store CUI | Process CUI | Transmit CUI | Not Applicable |
|-----------|-------------|--------------|----------------|
39. Describe how you would document the customer relationship, roles, and responsibilities between the ESP and the C3PAO environment (e.g., Customer Responsibility Matrix, Service Level Agreement, Vendor Placemat).
40. Describe how you are managing access for ESP employees to any CUI that may reside in the C3PAO environment.

CONTROLLED//PROPIN When Filled In
Candidate CMMC Third Party Assessment Organization (C3PAO)
Intake Form - TAB B

SECTION III: STAFFING INFORMATION

41. How many (W-2) employees are in the organization?
42. Does the organization use contractor (1099) employees?
43. How many (W-2) employees will have access to the C3PAO environment?
44. How many (1099) employees will have access to the C3PAO environment?
45. If the organization uses third-party service providers, how many of their employees will have access to the C3PAO environment?
46. How many employees (W-2 and/or 1099) will handle C3PAO-related CUI?
47. Does the organization have a filled, full-time Chief Information Officer (CIO) position?
48. Does the organization have a filled, full-time Chief Information Security Officer (CISO) position?
49. What duty position in the organization is responsible for the implementation of cybersecurity?
50. Describe how the business model supports separation of duties.

SECTION IV: C3PAO ENVIRONMENT

51. What is the version and date of the C3PAO environment's SSP?
52. How long has the C3PAO environment been operational?
53. What was the date of the most recent self-assessment for the C3PAO environment?
54. Does the organization have CMMC Level 2 practices that are not applicable (in full or in part)
If **YES**, please add those to TAB C.
55. Does the organization employ practices (in full or in part) that are inherited from another entity (e.g. cloud and/or managed service provider, enterprise)?
If **YES**, please add those to TAB C.

CUI Confirmation

56. Does/will CUI exist only within the scope identified previously in this section?
If **NO**, please provide an explanation in the comment section.

SECTION V: AUTHORIZED REPRESENTATIVE REVIEW AND VERIFICATION

The information on this form is accurate to the best of my knowledge. By signing the form below, I represent my full understanding and intention to make best efforts to maintain the scope for the assessment as referenced above.

Coordinating Official Signature and Date:

CONTROLLED//PROPIN When Filled In
Candidate CMMC Third Party Assessment Organization (C3PAO)
Intake Form - TAB B

CUI References:

- Executive Order 13556, November 4, 2010
<https://www.govinfo.gov/content/pkg/FR-2010-11-09/pdf/2010-28360.pdf>
- Part 2002 of 32 Code of Federal Regulations, September 14, 2016
<https://www.govinfo.gov/content/pkg/CFR-2018-title32-vol6/pdf/CFR-2018-title32-vol6-part2002.pdf>
- National Archives and Records Administration, CUI Registry
<https://www.archives.gov/cui>

CMMC References:

- CMMC Model 2.0 Overview, Version 2 December 2021
<https://dodcio.defense.gov/CMMC>
- CMMC Documentation
<https://dodcio.defense.gov/CMMC/Documentation>
- DoD Cybersecurity Toolbox (FedRAMP Equivalency - see Question #115)
<https://dodprocurementtoolbox.com/faqs/cybersecurity>
- FedRAMP Moderate Baseline documents
<https://www.fedramp.gov/documents-templates>
- FedRAMP Marketplace
<https://marketplace.fedramp.gov/#!/products>