A CVE Verified Service-Disabled Veteran Owned Small Business

C3PAO CMMC Assessment Questionnaire

Company Legal Name:	
Industry	
Primary Contact Name: **Title:** **Email:** **Direct Phone #:**	
Main Phone #:	
Headquarters Address:	
CAGE Code(s) included in CMMC Assessment Scope:	
Assessment Scope Enterprise or Enclave:	
Number of locations within the assessment scope: (If fully virtual, note this, and if any home office or alternate workplace has any infrastructure at it, e.g. company owned servers, routers, multifunction devices, etc.)	
Total # of Employees in your Organization?	
Total # of Authorized Users with access to your Assessment Scope environment?	
Total # of Computers with access to the Assessment Scope Environment?	
Is your assessment scope environment fully on-premise, hybrid, or fully virtual?	

Question	Yes	No	Not Applicable
Eligibility Questions			
Do you have an active direct contract with the Department of Defense?	○	○	○

KNC Strategic Services
701 Palomar Airport Rd, Suite 300, Carlsbad, CA 92011
(833) 562-7700 | www.kncss.com

KNC STRATEGIC SERVICES

A CVE Verified Service-Disabled Veteran Owned Small Business

If no, are you a subcontractor for a Prime with a DoD contract?	○	○	○
Do you currently store, transmit, or process any Controlled Unclassified Information (CUI) for DoD contract(s)?	○	○	○
Do you create CUI on behalf of the government ?	○	○	○
Have you implemented an ongoing Cybersecurity Awareness Training program?	○	○	○
Have all users who will be authorized to process, store, or transmit CUI completed the DoD Mandatory CUI training program?	○	○	○
How often do you conduct Cybersecurity Awareness Training?	○	○	○
Have those users completed training within the last 6 months on Insider Threat?	○	○	○
Have you completed a self-assessment of your environment against the NIST 800-171 controls and posted your score to SPRS?	○	○	○
Do you have an open Plan of Action & Milestones (POA&M) which outlines a timeline to complete remediation?	○	○	○
Do you develop software within your assessment scope?	○	○	○
SSP questions			
Do you have a completed System Security Plan (SSP)?	○	○	○
Was your SSP updated within the last 6 months?	○	○	○
Does your SSP describe how each Control/Practice and each Assessment Objective are met?	○	○	○
Do you have any controls listed as Not Applicable, and if you do, you have documented explanations as to why they are considered Not Applicable?	○	○	○
Do you have a Shared Responsibility Matrix for any Cloud Service Provider (CSP) and any External Service Provider (ESP) that you are inheriting any controls from?	○	○	○
If you are using a Cloud Service Provider (CSP) are they authorized as FedRamp Moderate?	○	○	○
If not, are they able to prove FedRamp Moderate Equivalency?	○	○	○
If using an External Service Provider (ESP) do they use one of your company-owned computers to access your Assessment Scope environment?	○	○	○
If you are using an External Service Provider (ESP), have they been	○	○	○

assessed by an Authorized C3PAO for meeting the requirements of NIST 800-171 or had a CMMC Level 2 Assessment completed?	○	○	○
If no, have they agreed in writing to support your assessment, including participating as needed in the assessment interview week?	○	○	○
Do you have a documented service level agreement for how the External Service Provider (ESP) agrees to meet the requirements according to the Shared Responsibility Matrix?	○	○	○
Policies Questions			
Do you have formal written policies based on, or covering, all of the NIST 800-171/CMMC control families?	○	○	○
Do you have employees, and anyone that is authorized to access your Assessment Scope environment, sign an Acceptable Use Policy, or an equivalent policy document?	○	○	○
Do you have all of your policy documents organized in a single repository?	○	○	○
Have all of your policy documents been reviewed, and updated as needed, within the last 12 months?	○	○	○
Procedures Questions			
Have you identified and documented all users (employees, contractors, third party vendors, ESP, and CSP) that are/will be authorized to process, store, or transmit CUI?	○	○	○
Have you identified who will be the primary Information Security Officer/Manager or equivalent?	○	○	○
Do you have and maintain a current Asset Inventory of all assets that will or may process, store, and transmit CUI?	○	○	○
Do you have each asset identified based on the appropriate CMMC Asset Category?	○	○	○
Do you have a current Data Flow Diagram?	○	○	○
Do you have a current Network Diagram?	○	○	○
Do you have an Assessment Boundary Diagram?	○	○	○
Do you have an Assessment Boundary document that describes your Assessment Scope environment?	○	○	○

KNC STRATEGIC SERVICES

A CVE Verified Service-Disabled Veteran Owned Small Business

CMMC Preparedness Questions			
Do you have remote access users?	○	○	○
If so, do they connect via VPN?	○	○	○
Do you manage the use of Privileged Accounts?	○	○	○
Do you allow BYOD (Bring Your Own Device) within your assessment scope?	○	○	○
Do you use Virtual Desktop Infrastructure within your assessment scope?	○	○	○
Has your Assessment Scope environment been in existence and in use for over 6 months?	○	○	○
If not, was your environment started and live within the last month?	○	○	○
Do you have any technology implementations, changes, or upgrades in process or planned?	○	○	○
Are you backing up sensitive data that is held within your Assessment Scope?	○	○	○
Are you conducting change control board meetings at monthly or quarterly to review any changes to your Assessment Scope environment?	○	○	○
Have you conducted a mock assessment of your Assessment Scope environment?	○	○	○
Have you implemented FIPS 140-2 validated encryption for all assets that store or transmit unencrypted CUI?	○	○	○

Additional Comments or Explanations

KNC Strategic Services
701 Palomar Airport Rd, Suite 300, Carlsbad, CA 92011
(833) 562-7700 | www.kncss.com