KNC STRATEGIC SERVICES

Authorized CMMC Third Party Assessment Organization (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 is Enterprise or Enclave:	
Number of locations within the assessment scope:	
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?	
Tentative Month and Year you are seeking an assessment?	

Eligibility Questions			
Question	**Yes**	**No**	**N/A**
Do you have an active direct contract with the Department of Defense?	☐	☐	☐
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 related 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?	☐	☐	☐
Do you conduct Cybersecurity Awareness Training at least annually?	☐	☐	☐
Have the CUI authorized 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 and or self-assessment?	☐	☐	☐
Do you have an open Plan of Action & Milestones (POA&M) which outlines a timeline to complete any open remediations?	☐	☐	☐
Do you develop software within your assessment scope?	☐	☐	☐
SSP questions			
Question	**Yes**	**No**	**N/A**
Do you have a completed System Security Plan (SSP)?	☐	☐	☐
Was your SSP updated within the last 12 months?	☐	☐	☐
Does your SSP describe how each Control and each Assessment Objective are met?	☐	☐	☐
Do you have any controls listed as Not Applicable, and if you do, 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) to process, store, or transmit CUI, are they authorized as FedRamp Moderate or higher?	☐	☐	☐
If not, are they able to prove FedRamp Moderate Equivalency?	☐	☐	☐
If you are using an External Service Provider (ESP), have they been assessed by an Authorized C3PAO for an official CMMC Level 2 Assessment?	☐	☐	☐
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			
Question	**Yes**	**No**	**N/A**
Do you have formal written policies based on, or covering, all 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 your documents/evidence organized in a single repository or in a GRC application?	☐	☐	☐
Have all your policy documents been reviewed, and updated if needed, within the last 12 months?	☐	☐	☐
Procedures Questions			
Question	**Yes**	**No**	**N/A**
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 in your assessment scope?	☐	☐	☐

Do you have and maintain a current Asset Inventory of all assets that are within your assessment scope?	☐	☐	☐
Do you have each asset identified based on the appropriate CMMC Asset Category? (CUI Asset, Security Protection Asset, Contractor Risk Managed Asset, etc.)	☐	☐	☐
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?	☐	☐	☐

CMMC Preparedness Questions			
Question	**Yes**	**No**	**N/A**
Do you have remote access users?	☐	☐	☐
If so, do they connect via VPN or other secure method?	☐	☐	☐
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 went live within the last month?	☐	☐	☐
Do you have any technology implementations, changes, or upgrades in process or planned in the near future?	☐	☐	☐
Are you backing up sensitive data that is held within your Assessment Scope to the cloud?	☐	☐	☐
Are you conducting change control board meetings 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 or higher validated encryption for all assets that store or transmit unencrypted CUI?	☐	☐	☐

Additional Comments or Explanations

Please explain the types of operating systems used for computers and servers, as well as the services you are using in your assessment scope (e.g., Microsoft GCC/GCC-High, AWS GovCloud, Google, Preveil, Kiteworks, NeqTer, etc.).