

iWorks provides consulting, assessment, remediation, monitoring, and maintenance services in support to your National Institute of Standards and Technology (NIST) 800-171 and Cybersecurity Maturity Model Certification (CMMC) journeys. Our approach begins by understanding your compliance requirements and desired maturity level to create a roadmap that leverages your current compliance stance in preparation for CMMC. If you need technical assistance in meeting the desired compliance level; we offer our highly qualified and certified technical staff to work with your team to address gaps in your cybersecurity posture. Finally, we help your organization institutionalize cybersecurity by providing ongoing advanced monitoring, incident response capabilities, vulnerability scan and analysis, intrusion detect and response, and advance threat preventions.

Please complete the cybersecurity questionnaire below to help us determine the level of effort and establish the roadmap required to achieve your desired cybersecurity posture.

- **Organizations Seeking Certification (OSC) Information**

Name: _____
Address: _____

- **OSC Coordinating Official**

Name: _____
Email: _____
Phone: _____

- **Targeted Cybersecurity Standard** (Select all that apply)

NIST 800-171 SPRS CMMC (Targeted level: 1,2,3,4,5) _____

- **Scope for the Assessment**

Do you own, process, or store Controlled Unclassified Information (CUI)?
 Yes No I don't know

- **Data location(s)** (Choose all that apply)

On-premises Cloud Hybrid Datacenter

- **Number of devices considered** (include network diagram if available)

Servers _____ Networking _____

- **Determine Software as a service (SaaS)** (Select all that apply)

Azure GCC Office 365 Other _____

- **Describe user authentication methodology** (e.g., On-prem AD)

- **Cybersecurity effort completed** (Select all that apply)

NIST 800-171 self-assessment SSP
 Defined security boundaries POAM

Please return completed form to CMMC@iworkscorp.com