

- MSP knows what CMMC stands for
- MSP is familiar with all controls in NIST 800-171 rev2, the DFARS 7012 Rule, and the timeline for CMMC
- MSP knows what CUI stands for
- MSP knows and how to identify CUI (or at least who to contact about CUI questions)
- MSP offers Shared Responsibility Matrix (SRM)
- MSP offers references of other CMMC Clients they are actively working with
- MSP has straightforward pricing structure
- MSP has asked and is clear about your current efforts towards compliance during the sales process
- MSP has clarity about “other costs” you may incur above the Agreement
- MSP does not say “we’ve got everything CMMC handled for you”
- MSP is clear whether they will facilitate the CMMC Program or you are responsible for facilitating the CMMC Program (facilitate vs. abdicate)
- MSP’s backup solution uses FIPS validated cryptography
- MSP’s recommended firewall as FIPS validated cryptography capabilities
- MSP knows the difference between FIPS validated cryptography and FIPS compliant cryptography
- MSP asks you about CUI/FCI flow (into organization, to whom, where stored, who accesses, for what, outflow, etc.) BEFORE recommending any solutioning
- MSP talks about the scope for applying the controls BEFORE recommending any solutions, performing a gap assessment, or making changes
- MSP discloses any contracted support services they utilize, foreign nationals working in their company, and/or any offshore staff
- MSP has delivered Letter of Intent to comply with NIST 800-171 and achieve CMMC Assessment and/or Certification at your required level or above
- MSP already has conducted their own Self Assessment, has a Plan of Action & Milestones (POAM), and (at least) draft Systems Security Plan (SSP)
- MSP utilizes MFA to access computers, M365/Google, and all toolsets that house or provide Security Protection Assets (SPAs) or Security Protection Data (SPDs)
- MSP can provide some evidence of their working towards compliance with CMMC
- MSP knows which vendors they use that will process, store, or transmit Security Protection Data and has vetted them to determine if they will be pursuing CMMC L2
- MSP has a MINIMUM of an RPA, CCP preferred
- MSP is involved with CMMC Industry groups

*Have confidence before tying yourself into a contract!*