Certified as a Registered Provider Organization (RPO) by The CMMC Accreditation Body (CMMC-AB)

CMMC PLANNING CHECKLIST

REVIEW CURRENT SYSTEM SECURITY PLAN (SSP)* AND ANY PLANS OF ACTION AND MILESTONES (POAMs)

* Must have in order to complete and submit your DoD NIST 800-171 Self-Assessment

SUBMIT YOUR DoD NIST 800-171 SELF ASSESSMENT

- Follow DoD scoring methodology
- Requires target date for full compliance

VERIFY LEVEL OF CMMC COMPLIANCE NEEDED AND ANY DIRECTION FROM PRIME

REVIEW OF CURRENT IT SYSTEMS

- Review of all IT tools and any shop floor machinery as applicable
- Determine if there are any changes required to meet CMMC practices and/or ITAR compliance

CONDUCT A NIST 800-171 AND CMMC GAP ASSESSMENT

- Detailed evidence collection of the following:
  - Existing policies/procedures
  - Existing IT environment
  - Existing physical security practices
- Audit entirety of evidence collected
- Identify/document gaps via Security Assessment Report (SAR) with Plans of Action and Milestones (POAMs)
- Determine timeline and budget required for remediation and ongoing support as needed

CHOOSE THE RIGHT PROVIDER

- Look for partners that have been verified by the CMMC-AB as a Registered Provider Organization (RPO).
- Look for partners that will be CMMC compliant. Managed Service Providers (MSPs) are required to be CMMC certified at the same level as their client as they are considered part of the supply chain.

Learn how SSE can help you assess and achieve compliance.

robert.duffy@SSEinc.com 314.439.4769