What You Need to Do

STEP 1 – Complete a CMMC Level 1 Self-Assessment
CMMC Level 1 consists of 15 cybersecurity measures, organized into six categories. These requirements are defined in the CMMC Scoping Guide Level 1 and the CMMC Assessment Guide Level 1. An excerpt from the DP3 Tender of Service listing these 15 measures is below.

c. The following basic safeguarding requirements and procedures are required to protect TSP information technology systems, including mobile applications, that process information received under the ToS program. IAW 48 CFR 52.204-1 and 32 CFR Part 170, these requirements and procedures for basic safeguarding of TSP systems shall include, at a minimum, the following security controls:

(1) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
(2) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
(3) Verify and control/limit connections to and use of external information systems.
(4) Control information posted or processed on publicly accessible information systems.
(5) Identify information system users, processes acting on behalf of users, or devices.
(6) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
(7) Sanitize or destroy information system media containing HHG ToS information before disposal or release for reuse.
(8) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
(9) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
(10) Monitor, control, and protect organizational communications (*i.e.*, information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
(11) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
(12) Identify, report, and correct information and information system flaws in a timely manner.
(13) Provide protection from malicious code at appropriate locations within organizational information systems.
(14) Update malicious code protection mechanisms when new releases are available.
(15) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

You must conduct a self-assessment against all 15 measures, documenting in a simple format *how* your company complies. The document should:

- List each control point
- Explain how your company meets the requirement
- Identify any policies, procedures, or tools used

This documentation must be retained in the event of audit. It does not need to be complex, but it **must exist**.

Additional official DoW guidance is available here: CIO - CMMC Resources & Documentation. And the IAM CMMC Resource page can be found here: IAM CMMC Resource Center - IAM.

STEP 2 – Record Compliance in SPRS
Once your self-assessment is complete, you must formally record your compliance in the **Supplier Performance Risk System (SPRS)**.

Important*: you should begin this process before/during your actual self-assessment process, as there is lead time involved in gaining access to the systems below*.

Required Step-by-Step Checklist

1. Register in SAM.gov (https://sam.gov/entity-registration), obtain a Unique Entity ID (UEID) and CAGE code, and ensure you have identified an "Electronic Business POC" in your SAM profile, as that must match the user you will eventually register for PIEE access (next step).
2. Once you have a CAGE code and EB POC, Register in the Procurement Integrated Enterprise Environment (PIEE). Request access to SPRS within PIEE. For PIEE assistance click Getting Started.
3. Assert your CMMC Level 1 certification in SPRS. Here is a link to the SPRS Quick Entry Guide - CMMCQuickEntryGuide.pdf.

Deadline and Enforcement

- Implementation deadline: 15 March 2026
- After that date:
    - Non-certified companies cannot participate in the DP3 supply chain
    - Prime contractors are prohibited from assigning DoD shipments to non-certified subcontractors
    - There are **no waivers or workarounds**