



# CMMC 2.0 COMPLIANCE

The Department of War (DOW) has implemented new standards for contractors to prove they have systems in place to protect digital and physical contract information. Known as the Cybersecurity Maturity Model Certification (CMMC), this is a safeguarding tool to ensure contractors **AND** subcontractors (at every tier) have consistent cybersecurity standards for processing, storing, and/or transmitting federal contract information (FCI) and controlled unclassified information (CUI). CMMC has 3 levels with various certification requirements. Levels 1 and 2 are described in the graphic below.

In November 2025, some contracts began requiring CMMC Level 1 and Level 2. By November 2026, some proposals and contracts will require CMMC Level 2 certification. Your CMMC status will need to be registered in the Supplier Performance Risk Systems (SPRS) to be eligible for these contracts.

Level 1: Foundation	Level 2: Self	Level 2: C3PAO
Essential cyber hygiene practices to protect Federal Contract Information.	Based on NIST SP 800-171 to protect Controlled Unclassified Information.	Based on NIST SP 800-171 to protect Controlled Unclassified Information.
<b>15 Requirements</b> FAR 52.204-21	<b>110 Requirements</b> DFAR 252.204-7012 DFAR 252.204-7020	<b>110 Requirements</b> DFAR 252.204-7012 DFAR 252.204-7021 DFAR 252.204-7025
<ul style="list-style-type: none"><li>Annual self assessment</li><li>Annual affirmation</li></ul>	<ul style="list-style-type: none"><li>Required prior to C3PAO certification</li><li>Annual affirmation</li></ul>	<ul style="list-style-type: none"><li>C3PAO certification assessment every 3 years</li><li>Annual affirmation</li></ul>

To ensure your ability to be part of future proposals, Bristol requests subcontractors obtain at least Level 1 certification. Once certified, register in SmartBid (link available on Bristol CMMC web page) and complete the Pre-Qualification process when you receive your confirmation email.



## Achieving CMMC Certification

### ONLINE RESOURCES

Department of War CMMC Website  
<https://dodcio.defense.gov/CMMC/>

Defense Logistics Agency  
Cybersecurity Resources for Suppliers  
<https://www.dla.mil/Small-Business/Resource-Center/Cybersecurity-Resources/>

NIST Computer Security Resource Center  
<https://csrc.nist.gov/>

NSA Defense Industrial Base (DIB) Cybersecurity Services  
<https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/DIB-Cybersecurity-Services/>

Project Spectrum  
<https://www.projectspectrum.io/#/>

SBA Strengthen Your Cybersecurity  
<https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity#best-practices-for-preventing-cyberattacks>

Supplier Performance Risk System  
<https://www.sprs.csd.disa.mil/>

### STEPS TO LEVEL 1 SELF CERTIFICATION

#### Step 1 - Register with these government systems:

- System for Award Management (SAM): <https://sam.gov/>
- Procurement Integrated Enterprise Environment (PIEE): <https://piee.eb.mil/>
- Supplier Performance and Risk System (SPRS): <https://www.sprs.csd.disa.mil/>

#### Step 2 - Review Systems & Security Requirements:

- Document all business systems (digital & hard copy) that are used to process, transmit, and store FCI: email, file storage, online workspaces, etc.
- Download and review required CMMC documents from Bristol website: <https://www.bristol-companies.com/subcontractors/cmmc/>:
  - CMMC Level 1 Self-Assessment Guide
  - Operational Plan of Action Memorandum (PoAM)
  - System Security Plan (SSP)
- Use the CMMC Level 1 Self-Assessment Guide to review and understand the 15 Security Requirements, such as: access control, identification & authentication, media protection, physical security, and basic cyber hygiene.

#### Step 3 - Conduct the Self Assessment

- Use the SSP to document your evidence of meeting each requirement: policies, screenshots, and configurations.
- Following the PoAM, evaluate each requirement and document whether it is Met / Not Met.
- Document any gaps and the remediation plan in the PoAM.
- Contact an approved assessor from the Cyber AB Marketplace for additional assistance:  
<https://cyberab.org/Catalog#!c/s/Results/Format/list/Page/1/Size/9/Sort/NameAscending>.

#### Step 4 - Record & Affirm in SPRS

- Log into the PIEE portal and access the SPRS module.
- Enter your score into the SPRS module.
- Annually assess and reaffirm compliance.

### LEVEL 2 CERTIFICATION

Bristol recommends that any subcontractor who seeks to obtain CMMC Level 2, work with an approved assessor from the Cyber AB Marketplace.