Bristol
ALLIANCE OF COMPANIES™

Bristol Alliance of Companies
111 W. 16th Avenue, Third Floor
Anchorage, AK 99501

Contracting Office
CMMC@bristol-companies.com

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, which are described below, that have various requirements for certification.

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 eligile for these contracts.

Level 1: Foundation

Essential cyber hygiene practices to protect Federal Contract Information.

15 Requirements
FAR 52.204-21

- Annual self assessment
- Annual affirmation

Level 2: Self

Based on NIST SP 800-171 to protect Controlled Unclassified Information.

110 Requirements
DFAR 252.204-7012
DFAR 252.204-7020

- Required prior to C3PAO certification
- Annual affirmation

Level 2: C3PAO

Based on NIST SP 800-171 to protect Controlled Unclassified Information.

110 Requirements
DFAR 252.204-7012
DFAR 252.204-7021
DFAR 252.204-7025

- C3PAO certification assessment every 3 years
- Annual affirmation

To ensure your ability to be part of future proposals, Bristol requests subcontractors obtain at least Level 1 certification. Once certified, complete the Cybersecurity Prequalification Questionnaire in SmartBid – https://securecc.smartinsight.co/#/PublicBidProject/854278.

Bristol
ALLIANCE OF COMPANIES™

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.