Supplier CMMC 2.0 Communication

The following information about the Department of Defense Cybersecurity Maturity Model Certification (CMMC) 2.0 is for information purposes only. Please follow the CMMC 2.0 regulation if there is any conflict.

Department of Defense (DoD) Cybersecurity Maturity Model Certification (CMMC) 2.0

Cybersecurity Maturity Model Certification (CMMC) 2.0

The Department of Defense (DoD) has introduced the Cybersecurity Maturity Model Certification (CMMC) 2.0 program, which streamlines cybersecurity requirements into three levels aligned with National Institute of Standards and Technology (NIST) standards. This program protects Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) shared with DoD contractors and subcontractors.

Key Definitions

- Federal Contract Information (FCI).: Information not intended for public release, provided by or generated for the Government under a contract.
- Controlled Unclassified Information (CUI): Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, subject to safeguarding or dissemination controls.

CUI Registry

The CUI Registry provides information on specific CUI categories and subcategories and can be accessed through the National Archives and Records Administration (NARA) and DoD websites.

Current Status

As of December 16, 2024, Title 32 CFR introduces the CMMC Program, requiring defense contractors to implement robust cybersecurity measures to protect FCI and CUI. Contractors must comply with specified CMMC levels, undergo assessments by Certified Third-Party Assessment Organizations (C3PAOs), and enhance their overall security posture to ensure supply chain compliance.

Under the rule, CMMC 2.0 assessments will be conducted by three distinct entities, depending on the certification level required:

- **CMMC Level 1** (Required for FCI)
  - Suppliers that do not process CUI must comply with CMMC Level 1, which establishes fundamental protection for FCI
  - POA&Ms are not permitted

BAE SYSTEMS

- CMMC Level 2 (Required for CUI): For suppliers handling Controlled Unclassified Information (CUI), CMMC Level 2 is the required certification level. :
    - Self -Assessment Conducted by Organization Seeking Assessment (OSA). Results uploaded to Supplier Performance Risk System (SPRS)
    - Assessment by CMMC Third Party Assessor Organization (C3PAO) every three (3) years. Results entered CMMC Enterprise Mission Assurance Support Service (eMASS)
- CMMC Level 3 Certification Assessments: (Required for CUI that requires additional protection as determined by the contract)
    - Assessment by Defense Contract Management Agency Defense Industrial Base Cybersecurity Assessment Center (DCMA DIBCAC)

Annual Self-Assessment and affirmation are required for all levels of CMMC; with relevant information uploaded to Supplier Performance Risk System (SPRS).

For further details, please visit the DoD CIO Website.

Additional Resources

The following list provides a detailed breakdown of the requirements under CMMC 2.0, designed to help suppliers thoroughly understand the specific security practices and processes necessary for compliance at each certification level.

- DIB SCC CyberAssist
    - DIB SCC CyberAssist is a cybersecurity assistance program for Defense Industrial Base (DIB) companies. It provides guidance and support to help companies comply with cybersecurity regulations and standards.
- DIB SCC CyberAssist CMMC
    - DIB SCC CyberAssist CMMC is an extension of the CyberAssist program, specifically focused on helping DIB companies achieve CMMC Levels 1-3. It offers resources and support for companies to prepare for and achieve CMMC compliance.
- Apex Accelerators
    - Apex Accelerators are a technology accelerator that provides resources and support to help small businesses CMMC compliance.
    - Please note that Apex Accelerators is not a CMMC certification body, but rather a partner that can help small businesses prepare for and achieve CMMC compliance.
- Project Spectrum
    - Project Spectrum is a DoD initiative aimed at improving the security and management of Controlled Unclassified Information (CUI). It provides a framework and tools to help DoD agencies and contractors manage CUI.
- DoD CUI Program
    - The DoD CUI Program is a DoD initiative that governs the handling and management of Controlled Unclassified Information (CUI) within the DoD. It establishes policies and

procedures for CUI classification, marking, and declassification, but it is not directly related to CMMC compliance.

- Redspin
  - Redspin is a CMMC Third Party Assessor Organization (C3PAO) and cybersecurity consulting firm that provides services such as vulnerability assessments, penetration testing, and compliance consulting. They help companies identify and mitigate cybersecurity risks and ensure compliance with regulations, including CMMC.
  - BAE Systems has negotiated beneficial pricing with Redspin for BAE Systems suppliers. Please contact Redspin for more details.

Should you have any questions, please contact your Cybersecurity-Supply Chain Risk Management (C-SCRM) Program Sector or Business Lead POC listed Below

BAE Systems, Inc	Bobby Fisher	bobby.fisher@baesystems.us
Intelligence & Security	Ashely Janiec	ashley.janiec@baesystems.us
Electronic Systems	Rebecca Barowski	rebecca.barowski@baesystems.us
Space & Mission Systems	Sarah Gray	sarah.gray3@baesystems.us
Combat Mission Systems	Kelly Coleman	kelly.coleman@baesystems.us
Combat Mission Systems- Cyber	Amber Fields	amber.fields@baesystems.us
Ship Repair	Toni Goehler	toni.puerile@baesystems.us
Ordnance Systems Inc. (OSI)	Colline Stevens	colline.stevens@baesystems.us
Weapons Systems- UK	Joel Hunt	joel.hunt@greenlnk.net
BAE Systems Hägglunds/Bofors	Mattias Halsius	mattias.halsius@baesystems.se