EMPOWERING OUR PARTNERS: NAVIGATING CMMC IN EUROPE

A Roadmap for Industry Compliance

Prepared Andy Cochran
Presented by Eric Thor

U.S. ARMY

US Army Corps of Engineers®

OUR STRATEGIC INTENT: EMPOWERING YOU

Independence through Information

- Cybersecurity is a shared global responsibility.
- Our goal today: Provide **you** with the knowledge, roadmaps, and official resources to pursue and achieve Cybersecurity Maturity Model Certification (CMMC) compliance.
- *USACE will not intermediate your certification process*; we are equipping you to take charge of your own readiness.
- Early adoption ensures your competitive advantage in future DoW procurements in the European theater.

CMMC IN THE EUROPEAN THEATER

Global Rules for the Defense Supply Chain

- What is CMMC? *A unified cybersecurity standard* for the entire Defense Industrial Base (DIB).
- Does it apply to European companies? YES. If you handle DoW data (FCI or CUI), CMMC applies regardless of your geographic location. COTS Exclusion: CMMC requirements do not apply to contracts, task orders, or delivery orders awarded solely for the acquisition of Commercial Off-the-Shelf (COTS) items.
- Can we use international auditors? Yes. The Cyber AB accredits Certified Third-Party Assessor Organization (C3PAO) globally. You are not restricted to US-based assessment firms; many provide international or remote services.

THE SPRS HUB & EXECUTIVE ACCOUNTABILITY

Shifting from Trust to Verification

- Supplier Performance Risk System (SPRS) is the DoW's authoritative source for your cyber scores.
- A firm’s SPRS-registered CMMC level must meet or exceed the solicitation’s CMMC requirement to be eligible for award.
- The Affirmation: CMMC eliminates "pencil-whipping." A Senior Official from your company must electronically sign an annual affirmation in SPRS.
- This makes compliance a legally binding corporate declaration subject to the False Claims Act.

KNOW YOUR DATA: FCI VS. CUI

Your data dictates your requirements

- Your required compliance level depends entirely on the data you handle.
- Federal Contract Information (FCI): Information not intended for public release. Requires CMMC Level 1.
- Controlled Unclassified Information (CUI): Sensitive information requiring strict safeguarding controls. Requires CMMC Level 2.

TWO DISTINCT GATES: SOLICITATION ACCESS VS. CONTRACT AWARD

The New USACE Procedures

- Gate 1: Accessing the Solicitation (Viewing Plans/Specs)
  - CMMC level status (Level 1/2) is NOT used as a criteria to view solicitation documents.
  - You DO need an active SAM.gov registration AND a valid NIST SP 800-171 self-assessment score (BASIC confidence level) posted in SPRS to download restricted, marked FCI/CUI attachments via the PIEE Solicitation Module.
- Gate 2: Winning the Contract Award
  - CMMC status IS a strict condition of contract award.
  - You must have your required CMMC level active in SPRS *prior* to award.

NAVIGATING CMMC LEVEL 1 (SELF-ASSESSMENT)

For contracts involving only FCI

- Requirements: 15 Basic Safeguarding Controls based on FAR 52.204-21.
- The Process (100% Self-Service):

1. Download the official DoD CIO Level 1 Assessment Guide.
2. Perform an internal self-assessment against the 15 controls.
3. Have a Senior Corporate Official submit the score and an Affirmation of Continuous Compliance into SPRS.
4. Repeat this affirmation annually.

NAVIGATING CMMC LEVEL 2 (CUI PROTECTION)

For contracts involving CUI

- Requirements: Additional controls based on NIST SP 800-171 Revision 2.
- Two Assessment Paths:
  - Level 2 (Self): You perform the assessment and enter the score in SPRS.
  - Level 2 (C3PAO): You must utilize an authorized Third-Party Assessment Organization to conduct an independent audit.
- Finding an Auditor: Visit The Cyber AB Marketplace to independently source and contract a C3PAO that services your European region.

NAVIGATING CMMC LEVEL 3 (HIGH-VALUE CUI PROTECTION)

For contracts involving CUI

- Focus & Purpose: Designed to safeguard critical or high-value Controlled Unclassified Information (CUI) against Advanced Persistent Threats (APTs).
- Security Requirements (134 Controls): Full compliance with 110 NIST SP 800-171 Rev. 2 requirements plus 24 enhanced controls from NIST SP 800-172.
- Strict Level 2 Prerequisite: Contractors must achieve a Final CMMC Level 2 (C3PAO) certification with all Level 2 POA&M items closed before a Level 3 assessment can begin.
- Audit Authority: Assessed every three (3) years exclusively by the DCMA DIBCAC with results submitted via CMMC eMASS into SPRS.
- Note: **Highly unlikely that Level 3 will apply to a construction contract**.

YOUR "SELF-HELP" TOOLKIT

The "Answer Keys" are public

- All necessary instructions are publicly available. Bookmark the DoD CIO Library: https://dodcio.defense.gov/CMMC/Resources-Documentation/
- Resources are available to answer your questions today:
  - Question: How do we isolate our networks to minimize audit scope and costs?
    - Answer: Download the Scoping Guides for detailed instructions.
  - Question: What are the exact criteria, interview questions, and testing methods used to pass every single control?
    - Answer: Consult the Assessment Guides for comprehensive details.
  - Question: How can we securely hash our proprietary evidence files to prove integrity during an audit?
    - Answer: Refer to the Artifact Hashing Guide for step-by-step guidance.

B2B COLLABORATION & PEER MENTORSHIP

Leveraging the European Defense Community

- Cybersecurity is a Team Sport: We strongly encourage our industry partners to network, exchange information, and share lessons learned regarding CMMC implementation in Europe.
- Peer Consulting: If your company has already successfully navigated the CMMC process or achieved certification, consider partnering with, mentoring, or consulting for other vendors who are just starting their journey.

B2B COLLABORATION & PEER MENTORSHIP

Leveraging the European Defense Community

- Prime/Sub Mentorship: Prime contractors are highly encouraged to actively mentor their subcontractors to ensure the entire supply chain remains eligible for future DoW awards.
- Disclaimer: *While USACE champions a strong, collaborative Defense Industrial Base (DIB), please note that the U.S. Government does not officially endorse, broker, or track private consulting arrangements.*

YOUR INDEPENDENT ACTION PLAN

Next steps for your organization

- Step 1: Upload your Basic NIST SP 800-171 score to SPRS immediately. You must have an active SPRS score on file to view marked FCI/CUI documentation and attachments in PIEE.
- Step 2: Download the official Assessment and Scoping Guides from the DoD CIO website.
- Step 3: Determine your required level based on the data you process (FCI vs. CUI) and identify your network boundaries.
- Step 4: Perform a gap analysis, remediate issues, and execute your self-assessment or contract a C3PAO.

OFFICIAL RESOURCES

Links to empower your journey

- DoD CIO CMMC Website: https://dodcio.defense.gov/CMMC/
- The Cyber AB (C3PAO Marketplace): https://cyberab.org/
- SPRS Help Desk: sprs-helpdesk@us.navy.mil or https://www.sprs.csd.disa.mil
- PIEE Access: https://piee.eb.mil
- USACE Europe District: https://www.nau.usace.army.mil/Business-With-Us/Contracting/
- Thank you for your partnership and commitment to securing our shared mission.