

DMAG 27 Feb 2026

Location: Embassy of Italy

Cybersecurity WG

Chair: Col J-F. Simard, Canada, jean-francois.simard3@forces.gc.ca

Co-chair: Mr. Stephen MacDonald, Canada

Member: Mr. Alex Berger, AUS

Member: Mr. Jack Beckman, UK



Updates



CMMC 2.0

- Phase I implementation (self assessment), until Nov 2026;
- WG is seeking engagements outside DoW, i.e., Cyber Accreditation Body (Town Hall on Mon 23 Feb), NDIA, AIA, etc., more to follow;
- Looking for additional WG members, Poland, Israel, Norway (non-5-Eyes)

Note: All questions or queries related to CMMC or any cybersecurity policies affecting the DMAG, please send to us.

CMMC Update (1/2)



- 32 CFR Part 170 Rule: Defines CMMC.
 - Published in the federal register and went into effect on December 16, 2024.
- **48 CFR 252.204-7021: Implements CMMC.**
 - Final rule posted to the Federal Register on 16 September 2025 and took effect 10 November 2025.
 - Will integrate CMMC requirements into the DFARS, specifically revises DFARS 252.204-7021.
 - Will allow DoD to incorporate CMMC requirements into DoD solicitations (RFIs and RFPs) and contracts.
- CMMC assessment requirements will be implemented using a four-phase plan over three years. The phases add CMMC Level requirements incrementally, starting with self-assessments in Phase 1 and ending with full implementation of program requirements in Phase 4.
 - Phase 1: Requires CMMC Level 1 or Level 2 self-assessments for certain contracts. The DoD does have discretion to include Level 2 certification assessment requirements into contracts during Phase 1. Starts on the effective date of the 48 CFR rule.
 - Phase 2: Requires official CMMC Level 2 assessments. Begins one year after Phase 1 starts.
 - Phase 3: Includes CMMC Level 3 assessments. Begins one year after Phase 2 starts.
 - Phase 4: Full implementation for all relevant contracts. Begins one year after Phase 3 starts.

CONCLUSION: DMAG member countries have until 10 November 2026 to prepare for CMMC Level 2 assessments and 10 November 2027 to prepare for CMMC level 3 assessments.

CMMC Update (2/2)



- DoD is offering three courses of action for foreign partner integration into CMMC:
 - COA 1: Existing authorized C3PAOs
 - Use existing accreditation body, Cyber AB.
 - Use existing Cybersecurity assessor and instructor certification organization (CAICO).
 - Add new foreign partner Certified CMMC Professionals and Certified CMMC Assessors.
 - COA 2: New authorized Foreign Partner C3PAOs
 - Use Cyber AB.
 - Use existing CAICO.
 - Add new foreign partner Certified CMMC Professionals and Certified CMMC Assessors.
 - COA 3: New foreign partner ecosystem:
 - Create foreign accreditation body.
 - Mutual recognition agreement between ABs.
 - Create new foreign partner C3PAOs accredited by foreign partner AB.
 - Use existing CAICO.
 - Use foreign partner CCPs and CCAs trained by U.S. CAICO approved ATP.
- New international partner C3PAOs:
 - ISO/IEC 17020 certified/compliant
 - Pass CMMC L2 assessment from DIBCAC