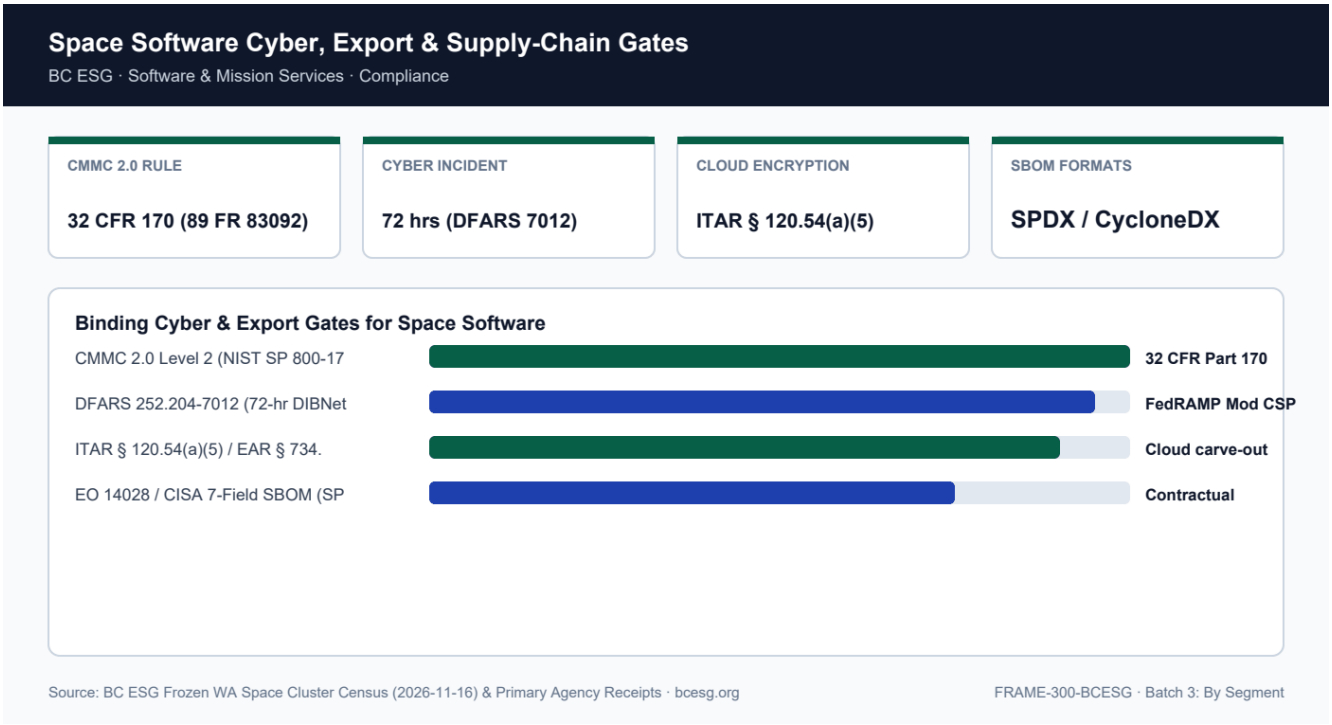
Software Compliance: CMMC 2.0 (32 CFR 170), DFARS 7012, ITAR Encryption & SBOM

Published: November 16, 2026 · Canonical URL: https://bcesg.org/wa-space-software-mission-services-compliance/

Verification & Scope Baseline: Binding DoD/export surface: 32 CFR Part 170 (CMMC 2.0), DFARS 252.204-7012 (72-hr DIBNet + FedRAMP Mod), ITAR § 120.54 / EAR § 734.18 encryption carve-outs, and EO 14028 SBOM.



Rule / Standard	Citation	Trigger	Mandatory Control
CMMC 2.0	32 CFR Part 170 (89 FR 83092)	FCI / CUI in DoD contracts	NIST SP 800-171 (110 controls) + SPRS/C3PAO
DFARS Cyber Reporting	48 CFR § 252.204-7012	Covered Defense Information (CDI)	72-hr DIBNet report, 90-day forensics, FedRAMP Mod
ITAR/EAR Cloud Safe Harbor	22 CFR § 120.54; 15 CFR § 734.18	Cloud storage/transit of tech data	E2EE FIPS 140-2/3, customer-held keys, no D:5
Software Bill of Materials	EO 14028 / CISA NTIA	Federal software procurement	7-field SPDX or CycloneDX + KEV tracking

Cybersecurity & Export Safe Harbors Replace Smokestack Permits

For Washington's 9 software and mission-services firms, environmental air/water permits are irrelevant—their binding compliance surface is **cybersecurity and export-controlled data custody**. Under **32 CFR Part 170 (89 FR 83092, CMMC 2.0)**, contractors handling Controlled Unclassified Information (CUI) must satisfy all 110 controls of **NIST SP 800-171 Rev 2** (with SPRS affirmations and C3PAO triennial assessments).

Under **DFARS 252.204-7012**, cyber incidents affecting Covered Defense Information must be reported to **DIBNet within 72 hours** with 90-day image/pcap preservation and **FedRAMP Moderate** equivalent cloud hosting. For cloud-hosted mission SaaS, **ITAR 22 CFR § 120.54(a)(5)** and **EAR 15 CFR § 734.18(a)(5)** provide the cloud encryption

carve-out—requiring end-to-end **FIPS 140-2/140-3** encryption with keys inaccessible to third-party/non-US cloud admins.

Verified Primary Sources & Internal Bridges

• Federal Register 32 CFR Part 170 (CMMC 2.0): https://www.federalregister.gov/documents/2024/10/15/2024-22921/cybersecurity-maturity-model-certification-cmmc-program

• eCFR DFARS 252.204-7012: https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-252.2/section-252.204-7012

• eCFR 22 CFR § 120.54 (ITAR): https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/section-120.54

• eCFR 15 CFR § 734.18 (EAR): https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-734/section-734.18

• CISA SBOM Framework: https://www.cisa.gov/sbom

• NTIA SBOM Minimum Elements: https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom