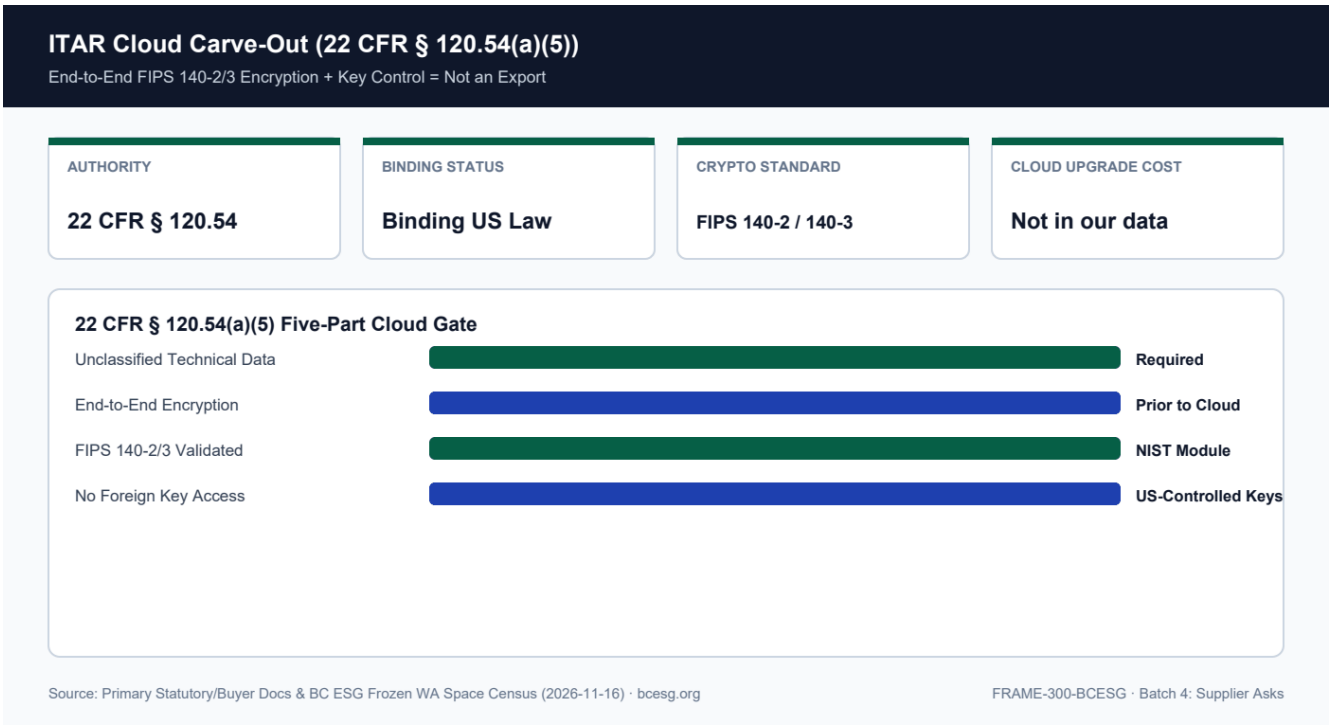
ITAR Cloud Storage & FIPS 140-2/3 Encryption (22 CFR § 120.54)

Published: November 16, 2026 · Canonical URL: https://bcesg.org/wa-space-ask-itar-cloud-fips-140-carveout/

Verification & Authority Baseline: Binding US federal regulation (22 CFR § 120.54(a)(5)). Storing or sending ITAR technical data over cloud/SaaS is NOT an export only when end-to-end encrypted using FIPS 140-2/3 validated cryptography with US-only access keys.



22 CFR § 120.54(a)(5) Criterion	What Auditors Check
End-to-End Encryption	Encrypted before leaving sender's boundary through rest/transit
FIPS 140-2 / 140-3	NIST-validated cryptographic module certificate
Key & Country Control	Cloud vendor cannot decrypt; zero storage in § 126.1 countries

Who Issues This Ask, Authority, and Binding Status

Cloud security questionnaires from primes and SaaS buyers ask WA suppliers whether their ERP, PLM, and file-sharing tools satisfy **22 CFR § 120.54(a)(5)**.

Binding status: `22 CFR § 120.54(a)(5)` is **binding US federal law** under ITAR. Without meeting all five criteria (unclassified data, end-to-end encryption, **FIPS 140-2/3** validated modules, no cloud-provider plaintext access, and no storage in proscribed `§ 126.1` countries), uploading ITAR CAD to a standard commercial cloud risks an unauthorized export.

Evidence Required & Small-Supplier Effort Cost

Suppliers document their **US Sovereign / GovCloud hosting** (e.g., Microsoft GCC High / Azure Government, AWS GovCloud) and **FIPS 140-2/3** key-management configuration inside their Technology Control Plan.

Licensing differentials between commercial cloud and GovCloud/GCC High are **not in our data**.

WA Space Cluster Segments & Companies Affected

Directly relevant to Software & Mission Services (Microsoft Azure Space, AWS Aerospace & Satellite, Integrate, M42 Space Engineering).

Verified Primary Sources & Internal Bridges

• eCFR — 22 CFR § 120.54 (Activities That Are Not Exports): https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/subpart-C/section-120.54