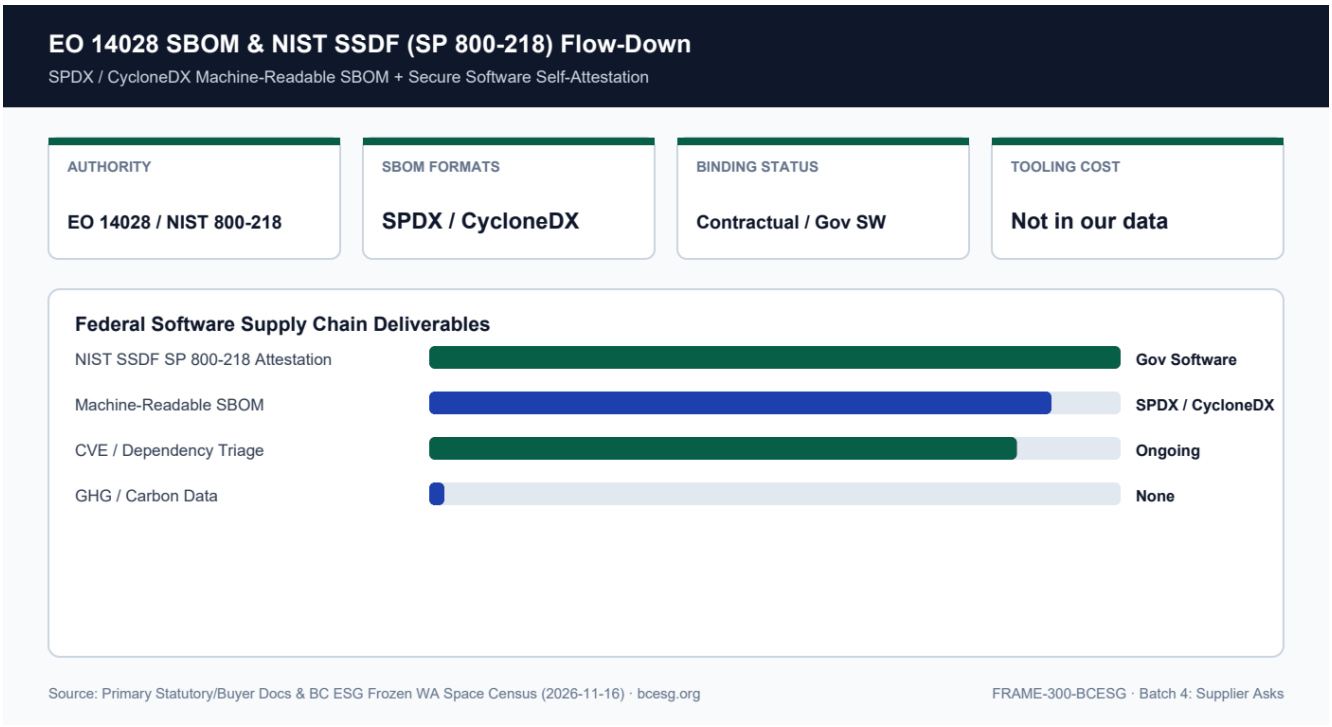
EO 14028 Software Bill of Materials (SBOM) & SSDF Attestations

Published: November 16, 2026 · Canonical URL: https://bcesg.org/wa-space-ask-eo-14028-sbom-software-attestation/

Verification & Authority Baseline: Issued by federal/DoD/NASA software buyers referencing EO 14028, NIST SP 800-218 (SSDF), and CISA SBOM formats (SPDX/CycloneDX). Binding only when incorporated via agency contract clauses or OMB M-22-18/M-23-16 agency acquisitions.



Artifact	Standard	Format
SBOM	CISA / NTIA Minimum Elements	SPDX (JSON/RDF) or CycloneDX (JSON/XML)
Developer Attestation	NIST SP 800-218 (SSDF)	Signed CISA/agency self-attestation form

Who Issues This Ask, Authority, and Binding Status

SBOM and Secure Software Development Framework (SSDF) attestation requests arrive from federal agencies, NASA, DoD primes, and mission-SaaS integrators buying flight, ground, or mission-management software.

Binding status: Executive Order 14028 and NIST SP 800-218 are **binding on federal software acquisitions** when written into contract clauses; for commercial-only space buyers, SBOMs remain a **voluntary / contractual** security deliverable.

Evidence Required & Small-Supplier Effort Cost

Suppliers generate a machine-readable **SBOM** in **SPDX** or **CycloneDX** format from CI/CD build pipelines and sign a **Secure Software Development Self-Attestation** mapped to NIST SP 800-218.

Open-source SBOM generators exist at $0 license cost; engineering hours for dependency remediation are **not in our data**.

WA Space Cluster Segments & Companies Affected

Affects Software & Mission Services (Integrate, Godel Space, M42 Space Engineering, Precursor SPC).

Verified Primary Sources & Internal Bridges

• NIST — SP 800-218 Secure Software Development Framework: https://csrc.nist.gov/pubs/sp/800/218/final

• CISA — Software Bill of Materials (SBOM): https://www.cisa.gov/topics/information-communications-technology-supply-chain-security/sbom