anchore

DoW Instruction (DoWI) 8430.01 makes SBOMs a condition to operate

If you build or deliver software for the Department of War (DoW), your next authorization conversation just changed. As of September 8, 2026, all software operated on DoW networks and systems needs **an SBOM and machine-readable proof of its build integrity and application security (§3.5.a(1)).** That's policy now, not a best practice. The instruction sets six requirements for your software supply chain. Here's what each one asks for, and how Anchore Enterprise meets it.

Who it covers

Every DoW Component and every program with software, acquisition or not, at any dollar value (§1.1.a). Contractors: expect it through your contract vehicle, and expect your vendor's SBOM to join your package.

Read the instruction

DoW Instruction (DoWI) 8430.01, Accelerated Mission Software. Approved by DoW CIO Kirsten A. Davies on August 31, 2026.

esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/843001p.pdf

Six requirements, and how Anchore Enterprise meets them

WHAT THE INSTRUCTION REQUIRES	HOW ANCHORE ENTERPRISE MEETS IT
1 **SBOMs for all covered software** Including open source, COTS, and transitive dependencies (§3.5.b)	Generate SBOMs at every build for container images, filesystems, and source. Import vendor SBOMs. Export in SPDX and CycloneDX formats.
2 **A secure, automated build** With machine-readable provenance (§3.5.c)	Verify signatures and provenance on your images. Your pipeline generates them. Anchore Enterprise doesn't sign.
3 **Scanning and compliance checks in CI/CD** Run continuously, not as final gates (§3.2.d)	Enforce policy in your pipeline with AnchoreCTL and block non-compliant images at Kubernetes admission. Policy packs cover DoD, STIG, NIST SSDF, FedRAMP, CIS, and CMMC.

WHAT THE INSTRUCTION REQUIRES	HOW ANCHORE ENTERPRISE MEETS IT
4 Continuous monitoring Of deployed software, with reporting of critical and actively exploited vulnerabilities (§3.5.h)	Re-evaluate stored SBOMs as vulnerability feeds update, so a new CVE is matched against every application without rescanning. Flag CISA KEV and EPSS data, and publish VEX.
5 Risk review of third-party and open source components Sustainment, security, and license obligations (§3.5.i)	Analyze components for zero-day vulnerabilities, malware, secrets, and open source license obligations. VEX annotations cut false positives.
6 AI-generated code tested like manual code With the AI components recorded (§3.6.c, §3.6.f)	Scan and enforce policy on dependencies an AI assistant introduces, like any other code. AI model artifacts such as GGUF files and Docker Models are detected in images and recorded in the SBOM.

Air-gapped environments

Deploy self-hosted on disconnected networks, with FIPS support, from IL2 through IL6. SBOMs and scan results stay on your network (§3.5.e).

Evidence on demand

SBOMs, findings, policy results, and VEX through the REST API, AnchoreCTL, and Anchore MCP. Standard evidence supports reciprocity (§3.4.d).

What you'll still need

Image signing and build provenance, plus SAST, DAST, fuzzing, and pen testing (§2.8.f). The authorization decision stays with your authorizing official.

Talk to our federal team about DoWI 8430.01.

go.anchore.com/contact