Verillian for Defense contractors

CMMC 2.0, NIST 800-171, ITAR

Controlled unclassified information cannot leak into a provider. Verillian enforces policy at the moment of execution and keeps the signing keys on the device, under your control.

$1.27M

Maximum ITAR civil penalty per violation, or twice the transaction value, and civil liability does not require intent. 22 CFR 127.10, effective 2025.

WHAT'S AT STAKE

When an employee pastes ITAR-controlled technical data or CUI into an AI tool, that export leaves your boundary with no record of what was disclosed, to which provider, or by whom. Civil ITAR liability does not require willful intent, so a single negligent disclosure is an enforceable per-violation event, and each transfer can be counted separately.

HOW VERILLIAN ANSWERS

Stop CUI before it leaves the device	Sensitive-data detection and redaction run on the device before any request crosses the boundary, so ITAR-controlled technical data and CUI are blocked or redacted rather than exported into a provider.
Policy enforced at execution	A sentinel governs any tool that speaks HTTPS to a provider, with no per-tool integration. Deny by default and fail closed mean that with no valid policy, AI traffic stops, matching NIST 800-171 and CMMC 2.0 access-enforcement expectations.
Tamper-evident evidence, keys on the device	Every interaction is signed on the device and hash-chained into an append-only record for non-repudiation. Signing keys never leave the device, giving defensible proof of what was and was not disclosed.
Self-hosted, zero-knowledge custody	Built for ITAR-regulated environments. The admin server stores only ciphertext under your own key, and Verillian retains none of your interactions, keeping CUI inside your control boundary.

Start a pilot. **verillian.ai**

Source: https://www.law.cornell.edu/cfr/text/22/127.10