Adopt AI on CUI without losing the contract

$1,271,078

Maximum ITAR civil penalty per violation, or twice the transaction value, whichever is greater. Liability is strict; no intent required. Source: 22 CFR 127.10.

THE EXPOSURE

- **CUI and ITAR data in prompts.** Controlled technical data pasted into AI tools leaves the boundary with no control and no record.
- **Shadow AI on engineering hosts.** Personal accounts, browser sessions, and command-line AI clients running outside any sanctioned route.
- **No evidence for the assessor.** Nothing to show under NIST 800-171 audit and accountability controls, or to satisfy a prime flow-down.

WHAT CHANGES WITH VERILLIAN

- **Decision before egress.** Policy is enforced when a tool acts, before content reaches a provider: allow, redact, or block.
- **Best-effort redaction at the device.** Outbound requests are scanned and redacted before leaving. Detection is best-effort, so it is paired with deny-by-default.
- **Your keys, your record.** Audit content is encrypted under a key only you hold. Verillian stores ciphertext it cannot read.
- **Assessment-ready evidence.** Every captured interaction is signed and hash-chained into a tamper-evident record an assessor can verify independently.

Built for CMMC 2.0 and NIST SP 800-171, mapped to the audit and accountability control family. Verillian is aligned to these requirements, not independently certified. Self-hosted and air-gapped capable, source-available under the Elastic License 2.0.

To see this on your own infrastructure, name a sponsor and a technical contact and we will scope a pilot in your environment, under your own keys.

hello@verillian.ai