

CI/CD PIPELINES

Every code change is automatically built, tested, security-scanned, and logged — so releases move from months to days, and the pipeline generates audit evidence as a byproduct, not a fire drill.

THE PROBLEM WE ADDRESS

Manual builds, emailed approvals, and quarterly "release weekends" mean finished capabilities sit undeployed for weeks or months while hard delivery dates slip.

Security scans run manually and inconsistently, assessment evidence is screenshots and emails, and change-control (CM-family) findings recur at every RMF assessment.

WHAT WE DO

- Current-state assessment of the software delivery lifecycle
- Pipeline architecture, platform selection, and environment promotion design
- Reusable pipeline templates committed to agency repositories
- Deployment automation with role-based approval gates
- SAST, SCA, secrets detection, and container image scanning as enforced gates
- SBOM generation per build (SPDX or CycloneDX)
- Pipeline logs and scan results routed to the agency's SIEM
- Control-mapping matrix tying each pipeline stage to NIST SP 800-53

HOW WE DO IT

1 ASSESS & DESIGN

Current-state review, tool and authorization constraints confirmed with the ISSM, and a pilot application selected.

DELIVERABLE

Target architecture + pilot selection

3 HARDEN & WIRE EVIDENCE

Security gates enforced, SBOM generation turned on, and the control-mapping matrix completed.

DELIVERABLE

Control-mapping matrix

2 BUILD

Pipeline-as-code, build and test automation, artifact management, and deployment jobs.

DELIVERABLE

Working pipeline-as-code

4 PILOT, TRANSFER & CLOSE

The pilot application runs through the pipeline in production use; runbooks, training, and a metrics baseline follow.

HANDOVER

Runbooks + metrics baseline

VALUE DELIVERED

- Audit evidence as a byproduct.** SBOMs and scan results are generated by every release, not assembled for the assessor after the fact.
- Built to survive Avalon's departure.** Role-based approval gates and trained developers/ISSM mean the pipeline doesn't depend on one or two people.
- Works with what you already licensed.** Avalon builds inside the agency's existing tooling rather than requiring a new procurement.
- Feeds your authorization evidence directly.** The control-mapping matrix is written for the SSP and the assessor, not just the developer.

THE ONE THING TO REMEMBER

Fixed price, fixed scope, a fast path to a proven pipeline.

COMMONLY PROCURED AS

CI/CD pipeline design & implementation services

AT A GLANCE

Model	Fixed price, fixed scope
Typical	10–12 wks for a standalone pipeline stand-up
NAICS	541512, 541511, 541519, 541611, 541690
UEI	Y9MXMMHY3HA1
CAGE	242T0
Standards	NIST SP 800-218 (SSDF), NIST SP 800-53, DoD DevSecOps Reference Design, FedRAMP 20x

WHO WE WORK WITH

- DevOps/platform lead whose releases depend on manual, undocumented steps
- ISSM facing recurring CM-family findings at every RMF assessment
- Program manager needing a licensed tool (Jenkins, GitLab) turned into a real pipeline

COMMITMENT TO QUALITY

Avalon is led directly by a PMP-certified founder with a decade of enterprise engineering experience where every engagement gets senior-level attention, never a subcontracted bench. Delivery follows NIST SP 800-53, RMF, and FISMA, evidence-backed and control-mapped by design. ISO 9001/27001 is on the roadmap as the pipeline scales.

Status: Small business federal contractor based in Los Angeles, CA

NIST SP 800-218 (SSDF)

NIST SP 800-53

DOD DEVSECOPS REFERENCE DESIGN

FEDRAMP 20X