

DEVSECOPS

Avalon builds security into how your software gets built, so your teams release updates in days instead of months, with the risk evidence your AO needs generated automatically.

THE PROBLEM WE ADDRESS

The Risk Management Framework was designed around systems that change slowly; modern software changes daily, and the mismatch produces the ATO bottleneck that leaves capabilities finished but undeployed.

ATO packages get assembled by hand from screenshots and spreadsheets, and POA&M backlogs grow faster than they burn down because continuous monitoring is neither continuous nor monitoring.

WHAT WE DO

- Pipeline architecture, toolchain, and security-gate coverage review
- Scored maturity baseline against the SSDF practice groups
- Sequenced remediation roadmap with effort estimates
- SAST, SCA/SBOM, secrets detection, container scanning, and DAST tuned as enforced gates
- Container hardening aligned to the DoD Container Hardening Guide and Iron Bank images
- Kubernetes policy enforcement, artifact signing, and secrets management
- Control-mapping matrix tying pipeline evidence to NIST SP 800-53 and SSDF
- Automated export of scan results, configuration state, and SBOMs to eMASS/Xacta/GRC

HOW WE DO IT

1 KICKOFF & ASSESSMENT

Interviews, pipeline and toolchain review, maturity scoring, and a prioritized roadmap.

DELIVERABLE

Maturity baseline + roadmap

3 SCALE & AUTOMATION

Templatized rollout to additional teams, policy-as-code, and evidence automation into the agency's GRC workflow.

DELIVERABLE

Scaled evidence automation

2 PILOT IMPLEMENTATION

Full security-gate and evidence build-out on one or two application teams' pipelines — the proof case.

DELIVERABLE

Hardened pilot pipeline

4 ENABLEMENT & TRANSITION

Training, security-champion designation, runbooks, and closeout.

HANDOVER

Trained security champions

VALUE DELIVERED

- › **Evidence built for the AO, not just the developer.** A dashboard is built for the ISSM and Authorizing Official specifically.
- › **No rip-and-replace.** Security engineering integrates into the pipeline your teams already use every day.
- › **Findings fixed at commit time.** Enforced gates with severity thresholds surface issues when they're cheapest to fix.
- › **An honestly independent assessment.** No incumbent O&M contract to protect means the review of your pipeline is genuine.

COMMONLY PROCURED AS

DevSecOps engineering & maturity transformation services

AT A GLANCE

Model	Fixed-price or T&M, scoped per engagement
Typical	4–9 months for a full transformation; 4–6 wks for the assessment alone
NAICS	541512, 541511, 541519, 541611, 541690
UEI	Y9MXMMHY3HA1
CAGE	242T0
Standards	NIST SP 800-218 (SSDF), NIST SP 800-53, DoD cATO Memo, FedRAMP 20x

WHO WE WORK WITH

- CISO / DevSecOps lead needing an ATO bottleneck resolved without slowing releases
- ISSM facing a growing POA&M backlog from inconsistent security scanning
- Program manager whose releases depend on scarce, siloed security talent

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 CATO MEMO

FEDRAMP 20X

THE ONE THING TO REMEMBER

No incumbent O&M contract to protect means an honest assessment of your pipeline.

