AVALON
TECHNOLOGY SERVICES

Securing Tomorrow's Missions Today.

★★★
2026

Bought the Scanners, Turned Off the Gates: A Fixed-Fee DevSecOps Gate and Supply-Chain Assessment for One Pipeline

DevSecOps: learn which security gates in your pipeline run, which ones stop a bad release, and what it takes to turn them on without stalling your developers.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary **2**

Why Pipelines Ship With the Gates Off **3**
Why It Concentrates in Government 3

The Mandates and the Calendar **4**

What the Assessment Does **5**
The Seven Gates and Four Levels 6
The SBOM Exposure Test 7
Deliverables 7
Where the Engagement Stops 7

Evidence the ISSM Can Use **8**

How an Engagement Runs **9**
What the Agency Provides 9
What Is Not Included 10

How Avalon Staffs It **10**

Pricing and How to Buy **11**

Illustration: One Program, Seven Gates **12**
Finding Age 13
Tuning Order 13
What the Engagement Costs 13

Common Pitfalls **14**

Conclusion and Next Step **14**

Appendices **15**
Appendix A: Glossary 15
Appendix B: Illustration Assumptions 16
Appendix C: References 16

Executive Summary

Most federal software programs already own security scanners. The licenses were bought, the tools were wired into the pipeline, and then the gates were set to warn instead of block because the first week of findings buried the developers. The program now pays for static analysis, dependency scanning and container scanning that produce reports nobody reads, and a release can still ship with a known exploited vulnerability inside it.

That gap has a clock attached. For civilian agencies, CISA Binding Operational Directive 26-04 (June 10, 2026) sets risk-based remediation clocks for known exploited vulnerabilities, starting at three days with forensic triage. A program that cannot say which deployed applications contain a vulnerable component cannot start that clock on time. In DoD, the continuous authorization (cATO) memo of February 2, 2022 asks for the same thing in a different form: security evidence produced by the pipeline, not assembled by hand before an assessment.

This paper is for the people who own that problem: program managers and PEO offices with a release schedule, CISOs and ISSMs who carry the vulnerability backlog, CIOs and CTOs who fund the follow-on work, and the CORs who buy it. It describes Avalon Technology Services' DevSecOps service, which starts with one engagement:

- **A fixed-fee gate and supply-chain assessment for one program's pipeline.** One unclassified program, about four to six weeks including kickoff. A scored baseline against NIST SP 800-218 (the Secure Software Development Framework, or SSDF) and the DoD Enterprise DevSecOps Reference Design; a gate-by-gate review of seven security gates; an SBOM exposure test against a current known exploited vulnerability; a control-mapping matrix for the ISSM; and a sequenced roadmap. The market band is $45K to $120K firm fixed price; Avalon prices this work at $45K to $75K.
- **A conditional pilot follow-on.** Gate engineering and tuning on one or two application teams' pipelines, priced separately from the roadmap.

Section 9 works through an illustrative program with 6 repositories and seven gate types. Every gate is licensed or approved, but only 17 of 40 gate slots run and 3 block a release: 93% of what the program paid for does not stop anything. The illustrative assessment fee is $60K.

The service engineers the pipeline and the evidence; the authorization decision remains the government's. Avalon does not issue or guarantee an ATO or a cATO, does not act as the independent assessor, and does not certify compliance.

Why Pipelines Ship With the Gates Off

The phrases below come up in almost every conversation about a federal pipeline. Each points to the same gap: tools were bought, but the engineering that makes them usable was not.

What the program says	What it usually means
"We bought the tools but the developers turned the gates off."	Gates were enforced before thresholds, suppression rules and an exception path existed
"Security findings show up at the end and blow the schedule."	Scans run after the build, outside the pipeline, or only before an assessment
"Our scans are manual and nobody looks at the results."	No owner, no severity threshold and no workflow for triage
"We just got told we need SBOMs for everything."	SBOMs are not generated per build, or are generated and never stored or queried
"Our POA&M backlog grows every quarter."	Findings are found faster than they are fixed, and old ones never age out

Why It Concentrates in Government

- **Tools and services are bought separately.** A license buy closes at fiscal year-end; the engineering to tune it is never funded.
- **Untuned gates slow delivery.** A gate that fails every build on low-confidence findings gets switched to warn-only within weeks, and nobody turns it back.
- **The incumbent builds the code.** Gate policy decisions sit between the developer, the ISSM and the program office, and nobody owns them.
- **Software assurance is now risk-based.** OMB M-26-05 (January 23, 2026) rescinded M-22-18 and M-23-16. Agencies set their own software assurance policies, so each program has to decide what evidence it needs rather than follow a single form.

The Mandates and the Calendar

Driver	What it says	What it means for this engagement
NIST SP 800-218 (SSDF)	Secure development practices in four groups: Prepare the Organization, Protect the Software, Produce Well-Secured Software, Respond to Vulnerabilities	The scoring backbone for the baseline; guidance agencies may use, not a government-wide mandate
OMB M-26-05 (Jan 23, 2026)	Rescinded M-22-18 and M-23-16; agencies set risk-based software and hardware assurance policies	The CISA secure software attestation form is optional and SBOMs are a contract term an agency may choose
CISA BOD 26-04 (Jun 10, 2026)	Risk-based remediation clocks for known exploited vulnerabilities, from three days with forensic triage to 14 days, 60 days or the next upgrade; replaced BOD 22-01 and BOD 19-02	The SBOM exposure test asks whether the program can confirm exposure inside those clocks
DoD cATO memo (Feb 2, 2022) and the DoD Enterprise DevSecOps Reference Design	Continuous authorization as an AO posture that is granted and can be revoked; a reference architecture for software factories	The baseline scores against the reference design; the AO decides whether ongoing authorization fits
DoD CSRMC (announced Sep 24, 2025)	The Cybersecurity Risk Management Construct; RMF, DoDI 8510.01 and eMASS remain in use	Pipeline evidence still lands in the program's existing RMF records
NIST SP 800-53 Rev. 5	SA, CM, SI, RA and SR family controls	The control IDs in the control-mapping matrix

Driver	What it says	What it means for this engagement
NIST SP 800-190, 800-204C and 800-161 Rev. 1	Container security, DevSecOps for microservices, supply chain risk management	Reference points for container, signing and provenance findings
OMB M-26-14 (May 2026)	A risk-based logging model; replaced M-21-31	Pipeline and platform audit logs are checked against the agency's logging decisions
FedRAMP Consolidated Rules (Jun 25, 2026)	Cloud offerings are "FedRAMP Certified" in classes A through D; certification covers the provider's offering only	Constrains which hosted scanning tools the agency can use; it does not certify a pipeline

Common triggers: a late or failed ATO, an incident traced to an unknown component (the Log4j pattern), an inspector general or GAO finding on vulnerability management, an SBOM request the program cannot answer, and fourth-quarter operations and maintenance funds in July through September 2027.

What the Assessment Does

A tool vendor's onboarding turns scanners on; a generic maturity survey scores the organization. Neither says which gates stop a bad release. This engagement works inside the agency's own toolchain (GitLab, GitHub, Jenkins or the agency-mandated equivalent) and installs nothing of Avalon's.

Step	Activities
Kickoff and access	Repository and pipeline read access agreed, government dependencies dated in writing, repositories in scope named and counted
Scored baseline	Interviews and pipeline review scored against SSDF practice groups and the DoD Enterprise DevSecOps Reference Design, using OWASP SAMM or DSOMM scoring
Gate review	Seven gates checked on every in-scope repository and tagged licensed, configured, enforcing or tuned
SBOM exposure test	A timed answer to "which deployed applications contain this component?" for a current known exploited vulnerability
Control mapping	Pipeline outputs mapped to 800-53 and SSDF requirements in a matrix the ISSM owns
Roadmap and readout	A dependency-ordered tuning list, a pilot scope and a briefing to the program office, CISO, ISSM and, where wanted, the AO

The Seven Gates and Four Levels

The gates reviewed are static analysis (SAST), software composition analysis with SBOM generation, secrets detection, container image scanning, dynamic testing (DAST) against test environments, infrastructure-as-code scanning, and artifact signing and provenance. Each gate on each repository is tagged at the highest level it reaches:

- **Licensed:** the tool is paid for or approved.
- **Configured:** the scan runs in the pipeline on every build.
- **Enforcing:** a failing result blocks merge or release.
- **Tuned:** documented severity thresholds, suppression rules and an exception workflow with a named approver exist.

Licensed versus enforcing is the budget number; enforcing versus tuned predicts whether developers switch the gate off again.

The SBOM Exposure Test

An SBOM is an operational asset, not a compliance document. The test picks a component from CISA's Known Exploited Vulnerabilities catalog and asks the program to say which deployed applications contain it. With SBOMs generated per build and stored where they can be queried, that is a two-hour answer. Without them it is a two-week hunt through build logs, and a civilian program on a three-day BOD 26-04 clock has already missed it.

Deliverables

Deliverable	Format
Maturity assessment report with scored baseline (SSDF and DoD Reference Design)	PDF or Markdown report and briefing deck
Gate coverage register: gate, repository, level, finding-age profile	Excel or CSV
SBOM exposure test record	Short memo with timings
Control-mapping matrix: pipeline evidence to 800-53 and SSDF	Spreadsheet, OSCAL-friendly columns
Target-state architecture and sequenced roadmap, with a pilot scope	Diagrams and a roadmap document

Where the Engagement Stops

The assessment stops at the control-mapping matrix. Exporting evidence into eMASS or a GRC tool and setting up ongoing authorization belong to Avalon's separate NIST RMF Implementation service. Build and deployment mechanics and delivery metrics such as lead time belong to the CI/CD Pipelines service, and Avalon quotes one or the other for a given pipeline, never both. The assessment does not rewrite application code, build landing zones (Cloud Architecture & Engineering and Cloud Migration & Development are separate services), run a penetration test, operate a security operations center or license tools.

Evidence the ISSM Can Use

Control	What the pipeline can evidence
SA-10, SA-11, SA-15	Developer configuration management, developer security testing and the development process and tools in use
CM-2, CM-3, CM-4, CM-6	Baselines as code, change control through merge requests, impact analysis and configuration settings
SI-2	Flaw remediation, with finding age by severity
SI-7	Software integrity through artifact signing and verification
RA-5	Vulnerability scanning coverage and frequency
SR-3, SR-4, SR-11	Supply chain controls, provenance and component authenticity through SBOMs and signing

The accurate way to state the value is narrow. The follow-on work implements and automates evidence for the SA, CM, SI, RA and SR family controls listed in the control-mapping matrix, reducing assessment preparation effort and supporting the system's continuous monitoring strategy. The assessment itself tells the ISSM which of those controls the pipeline can evidence today and which it cannot.

Accurate	Not accurate
A scored baseline against SSDF practices as of the review date	Achieves SSDF compliance or attestation
Evidence for the controls listed in the matrix	Delivers an ATO or a cATO
An input to the ISSM, the assessor and the AO	Speeds an ATO by a set percentage
A sequenced roadmap with a pilot scope	Guarantees passing an assessment

How an Engagement Runs

Phase	Timing	What happens
0: Kickoff and access	1–3 weeks	Accounts and repository access issued, dependency schedule signed, repositories named
1: Assessment and roadmap	3–5 weeks	Interviews, gate review, SBOM exposure test, control mapping, roadmap, five-business-day agency review, readout
2: Pilot (separate, conditional)	6–12 weeks	Gate engineering, tuning and an exception workflow on one or two teams' pipelines

What the Agency Provides

- One point of contact with authority, usually in the program office, who can unblock access and scheduling.
- Read access to repositories, pipeline definitions and scan results, with roles granted before kickoff. In DoD environments onboarding can take two to six weeks, so it is a dated government-furnished dependency in the statement of work.
- Four to eight hours a week from each participating team lead, and two to four hours a week from the ISSM or ISSO for evidence-format decisions.
- The current SSP, POA&M and prior assessment artifacts.
- A decision-maker with authority to approve gate policies, and a written direction to the incumbent developer to cooperate. Agency-caused delays move the schedule day for day.

What Is Not Included

Included	Separate work
Gate review and tuning plan	Gate engineering, unless bought as the pilot
Control-mapping matrix	GRC export, eMASS records and ongoing authorization
Pipeline scanning findings	A scoped penetration test under rules of engagement
Evidence the SSP author can use	Writing the SSP or the authorization package
Agency-owned tools	Tool licensing or resale
Pipeline security	Application rewrites, landing zones, SOC or incident response
Unclassified programs	Classified or cleared environments

How Avalon Staffs It

Avalon takes one engagement at a time, works business hours, and works on unclassified programs only. Avalon's founder serves as engagement lead, with one named, certified security engineer and a fractional compliance specialist, hired or subcontracted. Avalon has no past federal engagements under this service. FAR 15.305 says an offeror without a record of past performance may not be evaluated favorably or unfavorably on that factor; what protects the program is a named team, a fixed price and a bounded scope. Avalon never serves as the independent assessor of a pipeline it engineered.

Requirement	How it is handled
Security engineer	Named personnel whose certifications and investigation level match the agency's requirements, listed in the proposal
Privileged access on DoD systems	Personnel holding the DoD 8140 qualification the program requires, as a condition of the engagement
Civilian access	Public Trust investigation at the tier the agency requires
Platform	Work happens in the agency's own toolchain and platform, with access the agency provisions; Avalon hosts nothing
Findings handling	Agency-approved handling for scan output and SBOMs before award; nothing over unmanaged email
Insurance and contract vehicles	Any coverage the solicitation requires is a condition of award; Avalon does not hold a GSA Schedule or a governmentwide contract today

Pricing and How to Buy

Engagement	Market-norm range	Avalon
Pipeline assessment and roadmap, one program, 4–6 weeks	$45K–$120K	Firm fixed price, $45K–$75K; illustrative $60K
Pilot implementation, 1–2 application teams, Phases 0–2	$250K–$600K	Firm fixed price with named team and pipeline counts
Multi-team transformation, 3–6 teams	$750K–$2.5M	Not offered today

The assessment sits under the $350,000 simplified acquisition threshold and can be bought as an open-market purchase. Purchases between the $15,000 micro-purchase threshold and the SAT are generally set aside for small business when two or more capable small businesses are expected to compete. A pilot at the low end of its band can also fit under the SAT; larger work can be subcontracted to Avalon by a prime.

Avalon does not hold a GSA Schedule or a governmentwide contract today, and it does not resell tools.

Prices are fixed against named repositories, a named gate list and a dated dependency schedule. There is no performance-based fee.

Illustration: One Program, Seven Gates

The figures below are a planning illustration for one representative unclassified program with 6 repositories, 4 of which build container images. They are not a quote and not a result from any engagement.

Gate	Applies	Licensed	Configured	Enforcing	Tuned
Secrets detection	6	6	2	0	0
SCA with SBOM	6	6	4	1	1
SAST	6	6	5	1	0
Container image scanning	4	4	3	1	0
IaC scanning	6	6	2	0	0
Signing and provenance	6	6	0	0	0
DAST	6	6	1	0	0
Total gate slots	40	40	17	3	1

Every gate slot is licensed or approved, but 23 do not run at all and 14 run without blocking anything. Only 3 of 40 (8%) stop a release, and one is tuned. Signing runs nowhere and secrets detection runs on two repositories, and those are the two gates that matter most for supply chain exposure.

Finding Age

Age of open critical and high findings	0–30 days	31–90 days	91–180 days	Over 180 days	Total
Count	14	22	18	31	85

58% of open critical and high findings are older than 90 days. For a civilian program, any of these that appear in the KEV catalog are already on a BOD 26-04 clock.

Tuning Order

Wave	Gates	Why this order
1	Secrets detection; SCA with SBOM	Leaked credentials and vulnerable components are the fastest paths to exposure, and the SBOM answers the KEV question
2	SAST; container image scanning; IaC scanning	Thresholds and suppression rules agreed with developers before any gate blocks a merge
3	Signing and provenance; DAST	Signing needs a stable build; DAST needs a stable test environment

In every wave, thresholds and the exception workflow come before enforcement. A gate that blocks on day one without an exception path is the gate developers turn off.

What the Engagement Costs

Scope	Hours	Rate-band range	Planning fee	Inside $45K–$75K
Short (3-week Phase 1)	230	$39.0K–$52.5K	$46K	Floor applies
Base (4-week Phase 1)	300	$50.7K–$68.4K	$60K	Yes
Long (5-week Phase 1)	370	$62.5K–$84.2K	$73K	No: cap scope

The base case is a four-week Phase 1: 160 hours of lead and architect time at $185 to $250, 80 hours of security engineering at $145 to $195, and 40 hours of compliance support billed at the same engineer band (a planning assumption), plus 20 hours of lead time in Phase 0. That is 300 hours, or $50.7K to $68.4K, with a $60K planning fee at the midpoint. A three-week Phase 1 drops the low end to $39.0K, under the $45K floor, so the fee does not go below $45K. A five-week Phase 1 runs $62.5K to $84.2K; the top breaks Avalon's $75K band while staying inside the $45K to $120K market band, so the statement of work caps repositories instead. Every case sits far below the simplified acquisition threshold.

Common Pitfalls

Pitfall	How to avoid it
Pipeline work drifts into fixing application code	Name teams and repositories by count; code changes go to the development team
Platform work becomes infrastructure construction	Define the platform boundary in the statement of work
Evidence work becomes full package authorship	List evidence artifacts by name; GRC export and the package are separate
Access and onboarding slip silently	Dated government-furnished dependencies and explicit Phase 0 exit criteria
Enforcing gates before tuning them	Thresholds and exception workflow first, then enforcement
Quoting CI/CD and DevSecOps against one pipeline	One service per pipeline, one labor-rate table per proposal
Overselling the result	Engineer the pipeline and the evidence; the AO decides

Conclusion and Next Step

Owning security scanners is not the same as having security gates. What most programs lack is a count of which gates run and block, how old their findings are, and an order for turning gates on that developers will accept.

The natural first step is the fixed-fee gate and supply-chain assessment: one program's pipeline, about four to six weeks, under the simplified acquisition threshold, ending in a scored baseline, a gate coverage register, an SBOM exposure test, a control-mapping matrix and a sequenced roadmap. To discuss a program, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

SSDF
NIST SP 800-218, the Secure Software Development Framework: practices in four groups (PO, PS, PW, RV).

SBOM
Software bill of materials: a machine-readable list of the components in a build, in CycloneDX or SPDX format.

SAST and DAST
Static application security testing of source code, and dynamic testing of a running application.

Software composition analysis
Scanning third-party and open-source dependencies for known vulnerabilities and license issues.

KEV catalog
CISA's Known Exploited Vulnerabilities catalog, which drives remediation clocks under BOD 26-04.

Enforcing gate
A pipeline check whose failing result blocks a merge or release.

Tuned gate
An enforcing gate with documented thresholds, suppression rules and an exception workflow.

cATO
Continuous authorization to operate: an AO's authorization posture under the DoD memo of February 2, 2022.

Appendix B: Illustration Assumptions

All values are planning assumptions for one representative unclassified program. None is drawn from a specific agency, a real pipeline or a completed engagement.

Assumption	Value	Basis
Repositories	6, of which 4 build containers	Planning assumption
Gate state	17 configured, 3 enforcing, 1 tuned of 40 slots	Planning assumption
Open critical and high findings	85, 49 older than 90 days	Planning assumption
Assessment hours	160 lead, 80 security, 40 compliance, 20 Phase 0	Four-week Phase 1
Rates	$185–$250 lead; $145–$195 engineer and compliance	KB rate bands; compliance rate assumed
Price check	Base fee $60K	Inside $45K–$75K and $45K–$120K

Appendix C: References

1. **National Institute of Standards and Technology**, *SP 800-218, Secure Software Development Framework (SSDF) Version 1.1* https://csrc.nist.gov/pubs/sp/800/218/final
2. **National Institute of Standards and Technology**, *SP 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations* https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
3. **National Institute of Standards and Technology**, *SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations* https://csrc.nist.gov/pubs/sp/800/37/r2/final
4. **National Institute of Standards and Technology**, *SP 800-190, Application Container Security Guide* https://csrc.nist.gov/pubs/sp/800/190/final

5. **National Institute of Standards and Technology**, *SP 800-204C, Implementation of DevSecOps for a Microservices-based Application with Service Mesh*
https://csrc.nist.gov/pubs/sp/800/204/c/final

6. **National Institute of Standards and Technology**, *SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices*
https://csrc.nist.gov/pubs/sp/800/161/r1/final

7. **Department of Defense CIO**, *DoD Enterprise DevSecOps Reference Design and related documents*
https://dodcio.defense.gov/library/

8. **Department of Defense CIO**, *Continuous Authorization to Operate (cATO) memorandum, February 2, 2022*
https://dodcio.defense.gov/Portals/0/Documents/Library/20220204-cATO-memo-Signed-Cleared.pdf

9. **Akin Gump**, *Department of Defense Launches CSRMC, a New Cybersecurity Risk Management Construct*
https://www.akingump.com/en/insights/alerts/department-of-defense-launches-csrmc-a-new-cybersecurity-risk-management-construct

10. **Cybersecurity and Infrastructure Security Agency**, *Known Exploited Vulnerabilities Catalog*
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

11. **Tenable**, *CISA BOD 26-04 FAQ: Vulnerability Remediation Impact, June 11, 2026*
https://www.tenable.com/blog/cisa-bod-26-04-FAQ-vulnerability-remediation-impact

12. **Office of Management and Budget**, *M-26-05, Adopting a Risk-based Approach to Software and Hardware Security, January 23, 2026*
https://www.whitehouse.gov/wp-content/uploads/2026/01/M-26-05-Adopting-a-Risk-based-Approach-to-Software-and-Hardware-Security.pdf

13. **Office of Management and Budget**, *M-26-14, Ensuring Effective and Efficient Agency Logging and Network Visibility to Defend Against Evolving Cyber Threats, May 2026*
https://www.whitehouse.gov/wp-content/uploads/2026/05/M-26-14-Ensuring-Effective-and-Efficient-Agency-Logging-and-Network-Visibility-to-Defend-Against-Evolving-Cyber-Threats.pdf

14. **FedRAMP**, *FedRAMP program and 2026 Consolidated Rules*
https://www.fedramp.gov

15. **OWASP**, *Software Assurance Maturity Model (SAMM)*
https://owaspsamm.org

16. **OWASP**, *DevSecOps Maturity Model (DSOMM)*
https://dsomm.owasp.org

17. **Acquisition.gov**, *FAR 15.305, Proposal evaluation*
https://www.acquisition.gov/far/15.305

18. **Centre Law & Consulting**, *Inflation Updates to FAR Thresholds: What Changed on October 1, 2025*
https://centrelawgroup.com/blog/inflation-updates-to-far-thresholds-what-changed-on-october-1-2025/