



Securing Tomorrow's Missions Today.



The Release Weekend Is the Finding: A Fixed-Fee Pipeline Assessment and Target Design for One Application Team

CI/CD Pipelines: trace one code change from commit to production, learn which delays a pipeline can remove and which belong to change control, and get a fixed price for building it in the tooling you already own.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
Why Federal Releases Stay Slow	3
Why It Concentrates in Government	3
The Mandates and the Calendar	4
What the Engagement Does	6
Deliverables	8
Where the Engagement Stops	8
Evidence the ISSM Can Use	8
How an Engagement Runs	10
What the Agency Provides	11
What Is Not Included	11
How Avalon Staffs It	12
Pricing and How to Buy	13
Illustration: One Change, Commit to Production	13
Where the Days Go	14
What the Change Board Decides	15
What the Assessment Costs	15
Common Pitfalls	16
Conclusion and Next Step	16
Appendices	17
Appendix A: Glossary	17
Appendix B: Illustration Assumptions	17
Appendix C: References	18

Executive Summary

Most federal application teams already own a modern build tool. GitLab, GitHub Enterprise, Jenkins or Azure DevOps sits in the enterprise license, and releases still happen on a weekend, by hand, from a checklist one engineer keeps in their head. Security scans run the week before an assessment. The ATO evidence is a folder of screenshots. A one-line fix takes weeks to reach production, and nobody can say exactly where the weeks go.

Owning the tool is not the same as having the capability. A working pipeline builds, tests, scans and deploys every change the same way, enforces the approvals change control requires, and records each step as evidence.

This paper is for the people who carry that problem: program managers who own the mission software and the budget, CIO development and platform leads, ISSMs and ISSOs who must approve every tool, connection and gate, CISOs, and the CORs who buy the work. It describes Avalon Technology Services' CI/CD Pipelines service, which starts with one engagement:

- **A fixed-fee pipeline assessment and target design for one application team.** Three billable weeks after access is issued. Trace one code change from commit to production, baseline the four DORA delivery metrics, inventory the toolchain the agency already licenses and what the ISSM has authorized, and deliver a target pipeline architecture plus a fixed-price statement of work for building it. The market band is \$25K to \$50K firm fixed price; the illustrative fee is \$34K.
- **A separately priced stand-up follow-on.** A 10 to 12 week build of the pipeline as code for one to three named applications, with additional applications priced as options. The market band is \$120K to \$350K firm fixed price.

Section 9 works through an illustrative application. One change takes 40 calendar days from commit to production, but only 7.75 days of hands-on work (19% flow efficiency). 40% of the elapsed time sits in steps a pipeline can execute or record. 55% sits in the change board and the deployment window, which no tool fixes: that part needs a change-control decision by the government.

The service builds and documents. It implements automated enforcement and evidence for the controls the pipeline touches. The agency's assessor assesses those controls, and the Authorizing Official (AO) decides.

Why Federal Releases Stay Slow

The same phrases come up in almost every conversation about a federal application team's release process. Any two of them together usually mean the delivery path, not the code, is the constraint.

What the team says	What it usually means
"We deploy quarterly" or "release weekends"	Changes are batched because each release is expensive, which makes each release riskier
"Three weeks to get a one-line change to production"	Calendar time is spent waiting in queues, not in work
"The scans get run right before the assessment"	Security testing is an event, not a gate, so findings arrive late and in bulk
"Our ATO evidence is screenshots"	Change control happens, but nothing records it in a form an assessor can test
"We have GitLab but we're barely using it"	The license was bought; the pipeline engineering was never funded
"We keep getting written up on change control"	CM-family findings on baselines, approvals or access restrictions for change

Why It Concentrates in Government

- **Release knowledge lives in one person.** Contractor transitions and attrition leave the build steps undocumented, so each release depends on who is available that weekend.
- **Tools need authorization before they run.** Every scanner, runner and connection needs the ISSM's approval, and a pipeline designed without the ISSM stalls at week ten.
- **Change boards meet on a calendar.** A monthly CAB adds weeks to every change regardless of how fast the build is.

The Mandates and the Calendar

Driver	What it says	What it means for this engagement
NIST SP 800-53 Rev. 5	CM, SA, SI, RA, AU and SR controls on change control, developer testing, flaw remediation and supply chain	The control IDs each pipeline stage is mapped to
OMB M-26-05 (Jan 23, 2026)	Rescinded M-22-18 and M-23-16; agencies set risk-based software assurance policies	SSDF (SP 800-218) is guidance an agency may adopt; SBOMs are a contract term it may choose
NIST SP 800-218 and SP 800-204C	Secure software development practices and DevSecOps implementation guidance	Design references, not mandates; the pipeline produces SSDF-aligned evidence
DoD cATO memo (Feb 2, 2022)	Continuous authorization rests on ongoing monitoring, supply chain security and DevSecOps practice	An instrumented pipeline positions a program for continuous-authorization approaches; it does not achieve one
DoD CSRMC (Sep 24, 2025)	A new DoD cybersecurity risk management construct; RMF, DoDI 8510.01 and eMASS remain in use	Evidence is shaped for the authorization process the program actually uses
OMB M-26-14 (May 2026)	A risk-based logging model; replaced M-21-31	Pipeline event logs go to the agency SIEM according to the agency's logging decisions
CISA BOD 26-04 (Jun 10, 2026)	Risk-based remediation clocks for known exploited vulnerabilities; replaced BOD 22-01	A repeatable release path is how SI-2 fixes reach production inside the clock

Driver	What it says	What it means for this engagement
FedRAMP Consolidated Rules (Jun 25, 2026)	Offerings are "FedRAMP Certified" in classes A through D; certification covers the provider's offering only	SaaS pipeline tooling must be certified or hosted inside the system boundary

The engagement gets bought at predictable moments: an assessment or ATO renewal that produced CM-family or SI-2 findings; a hard mission date that development will hit but release logistics will miss; a cloud migration, where the new environment should start with a pipeline rather than inherit the old release process; leadership direction toward continuous authorization; an outage traced to a manual deployment; a contractor transition; and fourth-quarter funds, July through September, looking for a fixed-price, fast-start task.

What the Engagement Does

The assessment answers three questions for one application team: where a change spends its time between commit and production, what the agency already owns and has authorized, and what a pipeline built from those parts should look like. It works in the agency's tooling and does not select or buy new tools.

Step	Activities
Kickoff and access	Read access to repositories, tickets and change records agreed; government dependencies dated in writing; the pilot application and team named
Value-stream trace	One recent change followed from commit to production through review, build, test, scans, change board, deployment and evidence capture, with calendar and hands-on time per step
Metrics baseline	Deployment frequency, lead time for changes, change failure rate and time to restore, from the agency's own records
Toolchain and authorization inventory	What is licensed, what is installed, what the ISSM has authorized, and where SaaS tooling sits relative to the system boundary
Target design	Stages, environment promotion model, branching, secrets handling, runner placement, approval gates and separation of duties matched to the agency's change control policy
Stand-up SOW and readout	A fixed-price statement of work for the build, with per-application options, and a briefing to the program manager, ISSM and platform lead

Deliverables

Deliverable	Format
Current-state assessment with the commit-to-production trace	Markdown or PDF, with diagrams
DORA metrics baseline	Spreadsheet with method notes
Toolchain and authorization inventory	Spreadsheet
Target pipeline architecture	Markdown or PDF, with diagrams
Draft control-mapping matrix (pipeline stage to 800-53 control)	Spreadsheet, written for an SSP appendix
Fixed-price stand-up statement of work with per-application options	Word or PDF
Readout	Slide deck and live briefing

Where the Engagement Stops

The engagement does not select or procure security tools or design a security program (Avalon's separate DevSecOps service), refactor or containerize the application, write or fix test suites, or build the landing zone or Kubernetes platform the pipeline deploys into (Cloud Architecture & Engineering, Cloud Migration & Development). It does not write the SSP, run the assessment or facilitate the ATO; the control-mapping matrix is a handoff to whoever does. It does not resell licenses or operate releases after handoff.

Evidence the ISSM Can Use

A pipeline moves a set of controls from manually performed and manually evidenced to enforced in tooling and recorded automatically. The target design maps each stage to the controls it supports so the ISSM can see the contribution before anything is built.

Pipeline stage	Controls supported	What it records
Protected branches and enforced review	CM-2, CM-3, CM-5, SA-10	Baseline, change approvals and who can change what
Automated build with signed, versioned artifacts	CM-14, SI-7	Component signing and integrity checks
Automated test execution as a gate	SA-11, CM-4	Test results and change impact per release
SAST, dependency, secrets and container scanning gates	RA-5, SA-11, SA-15	Scan results against thresholds the ISSM approved
SBOM per build, where the agency requires it	SR-3, SR-4, CM-8	Component inventory and provenance
Approval-gated deployment	CM-3, CM-5	Separation of duties on production change
Pipeline logs to the agency SIEM	AU-2, AU-6, AU-12, CA-7	Audit records and a continuous monitoring feed
Repeatable release path	SI-2	Dated evidence of how fast fixes reach production

This paper names the matrix as a handoff and stops there. Turning pipeline evidence into an authorization package and ongoing monitoring is the subject of Avalon's separate NIST RMF Implementation service.

Accurate	Not accurate
Implements automated enforcement and evidence for CM, SA, SI, RA and AU controls	Makes the system compliant with NIST 800-53
Positions the program for continuous-authorization approaches	Achieves cATO
Produces SSDF-aligned development evidence and per-build SBOMs	Certifies SSDF conformance
Reduces assessment preparation for the controls the pipeline touches	Guarantees a clean assessment or speeds an ATO

How an Engagement Runs

Phase	Timing	What happens
Access lead	2–6 weeks, on the agency's clock	CAC or PIV, VPN and firewall approvals; the SOW ties the schedule to these dependencies
Trace and baseline	Week 1	Value-stream trace, DORA baseline, toolchain and authorization inventory
Target design	Week 2	Architecture, gates and promotion model worked through with the ISSM and the pilot team
SOW and readout	Week 3	Draft deliverables, five-business-day agency review, final briefing
Stand-up follow-on (separate)	10–12 weeks	Assess and design (1–2), build (3–7), harden and wire evidence (8–10), pilot, transfer and close (11–12)

What the Agency Provides

- A named pilot development team with four to eight hours a week, and one point of contact who can unblock access and scheduling.
- ISSM participation from week one, not week ten, for tool, connection and gate decisions.
- Access to repositories, tool licenses, change records and environments. Target environments are government-furnished.
- Direction to any incumbent contractor to cooperate with the trace and share release documentation.
- Account issuance written into the statement of work as a dated government-furnished dependency. Agency-caused delays move the schedule day for day.

What Is Not Included

Included	Separate work
Integrating scan tools the agency already approved	Selecting or procuring security tools
Running the team's existing tests in the pipeline	Writing or fixing test suites
Deploying to environments the agency provides	Building the landing zone or Kubernetes platform
A control-mapping matrix for the SSP author	Writing the SSP or the authorization package
Runbooks and training at handoff	Operating releases after handoff
Working in licensed agency tooling	License resale or hosted tooling
Unclassified environments	Classified or air-gapped environments

How Avalon Staffs It

Avalon takes one engagement at a time, works business hours, and works in unclassified environments only. Avalon's founder manages the engagement. The technical lead is one named, certified senior platform engineer, hired or subcontracted for the engagement and listed in the proposal; without that person confirmed, Avalon does not bid. 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 agency is a named lead, a fixed price and a bounded scope. Avalon never assesses its own work and will sign an organizational conflict of interest representation.

Requirement	How it is handled
Senior platform engineer	Named personnel whose certifications and investigation level match the agency's requirements, listed in the proposal, hired or subcontracted
Cloud, Kubernetes or toolchain credentials	Required on the named engineer where the agency's environment calls for them, as a condition of the engagement
DoD privileged access	A DoD 8140-qualified named engineer where the work needs privileged access, as a condition of award
Civilian and DoD access	Public Trust or other investigation at the level the agency requires, as a condition of the engagement
Hardened images	Where the agency's environment uses Iron Bank or other hardened images, the design uses them; Avalon has no onboarding of its own
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 target design, one application team, 3 billable weeks	\$25K–\$50K FFP	Firm fixed price; illustrative \$34K
Standalone stand-up, unclassified, 1–3 named pilot apps, 10–12 weeks	\$120K–\$350K FFP	Firm fixed price from the design, with per-app options
Pipeline line item inside a larger modernization or DevSecOps effort	\$60K–\$250K	As a subcontractor to the prime
Post-handoff support	Scoped hours pool	Business hours only; no response-time commitment

The assessment and the stand-up both sit under the \$350,000 simplified acquisition threshold, so both can be bought as open-market purchases. 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. Pipeline work inside a larger modernization task order can be subcontracted to Avalon by the prime. Avalon does not hold a GSA Schedule or a governmentwide contract today, and it does not resell licenses.

The stand-up is priced as a firm fixed base for the named pilot applications plus priced options for each additional application. Once the templates exist, a further application is days of work, not weeks, and an application with no automated tests or a fragile build is priced on its own line rather than absorbed. Labor categories carry the same rates across every line item.

Illustration: One Change, Commit to Production

The figures below are a planning illustration for one representative application team that releases through a monthly change board. They are assumptions, not measurements from any agency and not results from any engagement. A real trace replaces every number.

Step	Calendar days	Hands-on days	Share of lead time	Who can change it
Code review and merge	2	0.5	5%	Team practice
Manual build	1	0.5	2%	Pipeline can execute or record
Manual test cycle	8	3	20%	Pipeline can execute or record
Pre-release security scans	4	1	10%	Pipeline can execute or record
Change advisory board wait	15	0.25	38%	Change-control policy
Deployment window wait and release	7	1	18%	Change-control policy
Evidence capture (screenshots, tickets)	3	1.5	8%	Pipeline can execute or record
Total	40	7.75	100%	Flow efficiency 19%

Where the Days Go

Only 7.75 of the 40 days are work. The rest is waiting. The steps a pipeline can execute or record (build, test execution, scans and evidence capture) account for 16 days, or 40% of lead time. The change board wait and the deployment window account for 22 days, or 55%, and no pipeline changes them. Review and merge is 5%, and depends on team habits the pipeline can enforce but not create.

That split is usually the most useful finding in the readout. It tells the program manager which delays an engineering investment can address and which need a decision from the people who own change control. The manual test cycle only shrinks if automated tests exist, and writing them is the team's work.

What the Change Board Decides

Change board cadence	Average wait (days)	Lead time (days)	Policy-bound share
Monthly CAB (base)	15	40	55%
Biweekly CAB	7	32	44%
Weekly CAB	3.5	28.5	37%

Holding every other step constant, moving from a monthly to a biweekly board takes lead time from 40 to 32 days, and a weekly board takes it to 28.5. Even then, 37% of the time is policy-bound. Pre-approving standard changes that pass the pipeline's gates is a government decision; the pipeline produces the record that makes it defensible.

What the Assessment Costs

Scope	Rate-band range	Planning fee	Fits \$25K–\$50K
One app, 3 weeks (recommended)	\$27.9K–\$40.1K	\$34K	Yes
One app, 4 weeks	\$37.2K–\$53.4K	\$45K	No: cap scope
Two apps, 3 weeks	\$36.0K–\$51.2K	\$44K	No: cap scope

The base case is three billable weeks: a senior platform engineer full time at \$185 to \$260 an hour, a compliance specialist at one quarter time and a project manager at 10% to 15%, both at an assumed \$135 to \$185 (the knowledge base lists no separate rate for either). That is \$27.9K to \$40.1K, with a \$34K planning fee. A fourth week runs \$37.2K to \$53.4K, past the top of the band at the high rates. A second application adds a half-time infrastructure engineer, for \$36.0K to \$51.2K, also at the edge. So the recommended scope is one application, three weeks, with the two to six week access lead on the agency's clock.

For the stand-up follow-on, the knowledge base staffing (senior engineer at 0.75 to 1.0, infrastructure engineer at 0.5, compliance at 0.15 to 0.25, project manager at 0.1 to

0.15) over 10 to 12 weeks computes to about \$96K to \$205K in labor before per-application options. The firm fixed price is set from the target design and the named applications.

Common Pitfalls

Pitfall	How to avoid it
The pipeline becomes "fix the application"	Name application refactoring and test authorship as out of scope in the SOW
Application count creep	Name the pilot applications; price additional ones as options
Platform creep	Target environments are government-furnished; the landing zone is separate work
The ISSM arrives in week ten	ISSM in from week one; every gate agreed before it is built
Access issuance slips	Date it as a government-furnished dependency; the schedule moves day for day
License entanglement	Work only in licensed, authorized agency tooling; no resale
Inconsistent rates across line items	Same labor categories, same rates, in every line of a bundled proposal
Overselling the result	Use the accurate phrasing; the assessor assesses and the AO decides

Conclusion and Next Step

A release weekend is not a scheduling problem. It is a finding: the delivery path depends on manual steps, batched changes and evidence nobody records as it happens. Most agencies already own the tools to fix the engineering part. What they lack is a clear picture of where the time goes, which part belongs to change control, and a fixed price for building the pipeline in what they already have.

The natural first step is the fixed-fee pipeline assessment and target design: one application team, three billable weeks, under the simplified acquisition threshold, ending in a commit-to-production trace, a DORA baseline, a target architecture the ISSM has seen, a draft control-mapping matrix and a fixed-price statement of work for the stand-up. To discuss an application team, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

CAB

Change advisory board: the group that approves production changes under the agency's change control policy.

cATO

Continuous authorization to operate: a DoD approach, described in the February 2022 DoD CIO memo, that relies on ongoing monitoring and DevSecOps practice.

CI/CD

Continuous integration and continuous delivery: building, testing and preparing every change for release automatically, with deployment gated by defined approvals.

DORA metrics

Deployment frequency, lead time for changes, change failure rate and time to restore service, from the DevOps Research and Assessment program.

Flow efficiency

Hands-on work time divided by total elapsed time for a change.

Pipeline as code

Pipeline definitions stored and versioned in the repository alongside the application.

SBOM

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

SSDF

NIST SP 800-218, the Secure Software Development Framework.

Appendix B: Illustration Assumptions

All values are planning assumptions for one representative application team. None is drawn from a specific agency, a measured pipeline or a completed engagement.

Assumption	Value	Basis
Commit-to-production steps	Seven steps, 40 calendar days, 7.75 hands-on days	Planning assumption
Change board	Monthly, 15-day average wait; biweekly 7; weekly 3.5	Half the interval between meetings, rounded
Step classes	Pipeline can execute or record; team practice; change-control policy	Assigned per step for the illustration
Assessment staffing	Senior engineer 1.0, compliance 0.25, PM 0.10–0.15; second app adds 0.5 infrastructure	40 hours a week
Rates	Senior \$185–\$260; mid-level \$135–\$185 an hour	Market-norm estimates; compliance and PM assumed mid-level
Price check	Base fee \$34K	Inside the \$25K–\$50K band

Appendix C: References

1. **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>
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 800-218, Secure Software Development Framework (SSDF) Version 1.1*
<https://csrc.nist.gov/pubs/sp/800/218/final>
4. **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>

5. **National Institute of Standards and Technology**, *SP 800-190, Application Container Security Guide*
<https://csrc.nist.gov/pubs/sp/800/190/final>
6. **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>
7. **Department of Defense CIO**, *DoD CIO Library, including the DoD Enterprise DevSecOps Reference Design*
<https://dodcio.defense.gov/Library/>
8. **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>
9. **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>
10. **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>
11. **FedRAMP**, *FedRAMP program and 2026 Consolidated Rules*
<https://www.fedramp.gov>
12. **DevOps Research and Assessment**, *DORA research program and metrics*
<https://dora.dev>
13. **Acquisition.gov**, *FAR 15.305, Proposal evaluation*
<https://www.acquisition.gov/far/15.305>
14. **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/>