



Securing Tomorrow's Missions Today.



Build Before You Bet: A Fixed-Fee Cloud-Native Discovery Sprint for One Mission Service

Cloud Native Development: scope, size and price one new mission service before committing build money

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
Why Cloud Builds Stall Before They Start	3
Why It Concentrates in Government	3
The Mandates and the Calendar	5
What the Discovery Sprint Does	7
Deliverables	9
Where the Engagement Stops	9
Evidence the ISSO Can Plan Around	9
How an Engagement Runs	11
What the Agency Provides	11
What Is Not Included	12
How Avalon Staffs It	12
Pricing and How to Buy	13
Illustration: Sizing One MVP by Its Integrations	14
What Waiting Costs	14
What the Sprint 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

Many federal programs already have a modernization roadmap. What they lack is working software. The roadmap names a target architecture, a cloud platform and a delivery date, and then the build money is committed before anyone has counted the integrations, confirmed the authorization pathway with the ISSO or written down what the first release must do. Month four arrives, the government expected the full legacy feature set, and the schedule resets.

Cloud native development builds a new mission service, or replaces one outright, using containers or managed services, infrastructure defined as code and an automated pipeline that tests and scans every change. Done well, the agency owns the code, the infrastructure definitions and the pipeline, and can change the system safely in days. Done badly, it is a cloud-hosted monolith with a larger bill. The difference is usually decided before the first line of code, in how the build is scoped.

This paper is for the people who fund and gate that build: program managers and system owners who own the mission problem, CIOs who set platform standards, CISOs and ISSOs who approve the pipeline and the evidence approach, and the CORs who buy and manage the work. It describes Avalon Technology Services' Cloud Native Development service, which starts with one engagement:

- **A fixed-fee discovery sprint for one mission service.** One unclassified service, two to four weeks of work (six at most). User and integration inventory, data classification and impact level, the authorization pathway confirmed with the ISSO, a rebuild-versus-refactor recommendation, a reference architecture, a signed MVP scope statement, a prioritized backlog and a priced build roadmap. The market band is \$50K to \$150K; Avalon prices this work at \$45K to \$85K firm fixed price.
- **A conditional build follow-on.** A steel thread and iterative MVP build in the agency's own environment, priced separately against the signed scope.

Section 9 sizes an illustrative MVP by its named integrations. With two legacy integrations the build runs about 20 weeks and \$594K to \$702K; with six it runs 36 weeks and up to \$1.26M, past the small-system band. The illustrative sprint fee is \$53K.

Avalon builds, hardens and documents; final certification or authorization rests with the appropriate government body. Avalon does not issue or guarantee an ATO, does not assess its own work, and does not certify compliance.

Why Cloud Builds Stall Before They Start

The phrases below come up in almost every conversation about a mission system that needs replacing. Each points to a scoping gap, not a technology gap.

What the program says	What it usually means
"We have a modernization roadmap."	A document exists and software does not; nobody priced the first release
"A change that should take a week takes a quarter."	Releases are batched twice a year, so an approved change waits months to ship
"We lifted and shifted and our cloud bill went up."	The system moved but its architecture did not; it runs at peak size all the time
"Only the incumbent can touch it."	Source, build steps and integrations are undocumented, so every change carries risk
"The ATO takes longer than the development."	Evidence is assembled by hand at the end instead of produced by the pipeline
"It fell over during open enrollment again."	The system cannot scale for a surge without re-engineering

If the real need is to move what exists, that is Avalon's separate Cloud Migration & Development service. If it is to fix a system the agency will keep (roughly half or more of the code retained), it is Application Modernization. This service applies when the answer is a new service or an outright replacement.

Why It Concentrates in Government

- **Build money arrives before scope does.** Annual appropriations push programs to obligate a large build in one action, before integrations are counted.
- **Integrations dominate cost, and nobody counts them.** A system with five undocumented interfaces takes longer than a larger one with clean APIs.
- **Access takes weeks.** CAC or PIV issuance, VPN, cloud accounts and government laptops routinely take two to eight weeks, and a paid team waits.

- **Authorization is planned last.** If the ISSO first sees the pipeline in month five, the evidence approach is rebuilt in month six.

The Mandates and the Calendar

Driver	What it says	What it means for this engagement
NIST SP 800-53 Rev. 5 and SP 800-37 Rev. 2	Controls and the seven-step RMF, including Prepare	The sprint names the developer-owned controls the build will evidence; the agency's RMF process authorizes the system
NIST SP 800-53 SA-22	Unsupported system components must be replaced or justified	SQL Server 2016 support ended July 14, 2026; Windows Server 2016 ends January 12, 2027. A rebuild retires these findings
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; the CISA attestation form is optional; an SBOM per build is a contract term the 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	Container base images must be rebuildable inside those clocks for civilian systems
OMB M-26-14 (May 2026)	A risk-based logging model; replaced M-21-31	Sets what the application logs under AU-2 and AU-12
FedRAMP Consolidated Rules (Jun 25, 2026)	Offerings are "FedRAMP Certified" in classes A through D; certification covers the provider's offering only	The agency's custom system is authorized under its own RMF process and inherits controls from the certified platform

Driver	What it says	What it means for this engagement
Section 508 and the 21st Century IDEA Act (2018)	The 2017 508 refresh incorporates WCAG 2.0 AA; WCAG 2.1 and 2.2 are current W3C guidance	Accessibility is scoped in discovery and tested every sprint, not at the end
DoD cATO memo (Feb 2, 2022) and CSRMC (announced Sep 24, 2025)	Continuous authorization as an AO posture; RMF, DoDI 8510.01 and eMASS remain in use	For DoD builds, the AO decides whether continuous authorization fits; the sprint only records the AO's posture

Common triggers: a stalled modernization program, an end-of-support date, a new statutory requirement the legacy system cannot absorb, an inspector general finding, an incumbent contract expiring within 12 to 18 months, and fourth-quarter funds in July through September 2027. FY2028 budget justifications, prepared in spring 2027, need a priced build roadmap to request the money.

What the Discovery Sprint Does

The sprint is Phase 0 of a cloud native build, sold on its own. It produces the artifacts the agency needs to fund, compete and govern the build, and the agency keeps them whoever builds. Work happens in the agency's own repositories and collaboration tools.

Step	Activities
Kickoff and access	Product owner named, government dependencies dated in writing, repository and document access agreed
Users and mission outcome	Interviews with users and stakeholders; the outcome the first release must deliver, in plain terms
Integration inventory	Every system the service must exchange data with, by name, with interface type, documentation state and owner
Data and authorization pathway	Data types (PII, PHI, CUI), impact level, hosting platform and the authorization pathway, confirmed with the ISSO
Rebuild or refactor	A written recommendation where a legacy system exists, with the share of code expected to be retained
Architecture	A reference architecture sized to the problem: a modular monolith, managed containers, Kubernetes or serverless on the agency's platform
Scope, backlog and roadmap	A signed MVP scope statement, a prioritized backlog, and a priced build roadmap with integrations as separate line items

Deliverables

Deliverable	Format
Integration inventory and data classification	Spreadsheet in the agency's repository
Rebuild-versus-refactor recommendation	Short memo
Reference architecture and architecture decision records	Diagrams and Markdown, in-repo
Developer-owned control list and evidence plan for the ISSO	Spreadsheet mapped to the agency's SSP structure
MVP scope statement, signed by the product owner	Document
Prioritized backlog	In the agency's backlog tool
Priced build roadmap with optional integration line items	Roadmap document and cost table

Where the Engagement Stops

The sprint writes no production code and builds no environment. Landing zones and account structure belong to Avalon's Cloud Architecture & Engineering service; moving existing workloads to Cloud Migration & Development; retaining and refactoring a system to Application Modernization; choosing which systems in a portfolio to retire or replace to IT Modernization; and a pipeline bought as its own product to the CI/CD Pipelines and DevSecOps services. The sprint does not write the SSP, run the ATO process, penetration test anything, operate the system or resell licenses.

Evidence the ISSO Can Plan Around

A cloud native build produces evidence for the controls a developer owns. The sprint names those controls for this service, so the ISSO knows in week three what the build will hand over in month five.

Control	What the build evidences
CM-2, CM-3, CM-6	Baselines and configuration defined as code; change control through reviewed merge requests
SA-11(1), SA-15	Static and dependency analysis in the pipeline; a documented development process and toolset
SA-22	Unsupported components removed by design
SI-2, SI-7, SI-10	Flaw remediation by rebuild; signed images; input validation in the application
RA-5	Scanning on every build, feeding the agency's vulnerability process
AU-2, AU-12	Audit events instrumented in the application and sent to the agency's logging stack
IA-2, AC-3, AC-6	Agency identity integration (PIV under FIPS 201) and least-privilege authorization
SC-8, SC-13, SC-28	FIPS-validated encryption in transit and at rest
CP-10, SR-4	Recovery by declarative rebuild; an SBOM per release where the contract asks for one

The accurate statement of value is narrow: the build delivers the system with pipeline-integrated security testing, hardened baselines, SBOMs and control implementation narratives for developer-owned controls, reducing the assessment and authorization effort that follows.

Accurate	Not accurate
A named list of developer-owned controls and an evidence plan	Delivers an ATO or an ATO date
Narratives the SSP author can use	A "FedRAMP Certified application"
Accessibility tested every sprint	"508-certified"
Inputs to the ISSO, the assessor and the AO	Continuous authorization the AO has not adopted

How an Engagement Runs

Phase	Timing	What happens
0: Discovery sprint (this offer)	2–4 weeks, 6 at most	Inventory, pathway, architecture, signed MVP scope, priced roadmap, five-business-day agency review, readout
1: Steel thread (separate)	3–6 weeks	One end-to-end slice deployed through the pipeline with security gates; the ISSO sees the pipeline
2: Iterative build (separate)	3–9 months	Two-week sprints, each ending in a demonstration of deployed software
3: Hardening and evidence	4–8 weeks, overlapping	Load testing, scan remediation, 508 audit, control narratives and SBOMs to the ISSO
4: Transition	2–4 weeks	Runbooks, recorded walkthroughs and paired sessions with agency staff or the sustainment team

What the Agency Provides

- A named product owner with decision authority, at 25 to 50 percent of their time. This is the strongest single predictor of a successful build.

- The ISSO from the first week, for two to four hours a week, to confirm the authorization pathway and evidence format.
- Access to users and to each integration's system owner, with interface documentation and test credentials where they exist.
- Repository, document and collaboration access issued before kickoff. Access delays are dated government-furnished dependencies in the statement of work, and they move the schedule day for day.
- Existing architecture documents, the current SSP if one exists, and any prior modernization studies.

What Is Not Included

Included	Separate work
Reference architecture	Landing zone, account structure and network design
Priced build roadmap	The build, unless bought as a follow-on
Developer-owned control list	The SSP, the ATO process and engagement with the AO
Rebuild-versus-refactor memo	Refactoring or migrating an existing system
Agency tools and repositories	License resale or tooling of Avalon's own
Unclassified, non-IL5 services	Classified, IL5 or IL6 work

How Avalon Staffs It

Avalon takes one engagement at a time, works business hours, and works on unclassified, non-IL5 systems only. Avalon's founder serves as engagement manager. The sprint is led by one named cloud architect with a current AWS or Azure professional certification, or a CKA or CKAD, hired or subcontracted and listed in the proposal, with a fractional DevSecOps engineer and compliance liaison. 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 fixed price, a bounded scope, key-personnel terms and artifacts that live in the agency's repositories from day one.

Requirement	How it is handled
Cloud architect	Named personnel whose certifications and investigation level match the agency's requirements, listed in the proposal
Civilian access	Public Trust investigation at the tier the agency requires
Build team for a follow-on	Named engineers, hired or subcontracted per engagement and listed in the build proposal
Platform and tools	The agency's repositories, backlog tool and cloud tenancy; Avalon hosts nothing
Data rights	Government-purpose or unlimited rights in everything produced; no Avalon-retained code
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
Discovery sprint, one service, 2–4 weeks (6 at most)	\$50K–\$150K	Firm fixed price, \$45K–\$85K; illustrative \$53K
MVP build, small system, 4–6 months	\$450K–\$1.2M	Priced against the signed scope, as a subcontractor or through a competed action
Mid-size build with integrations, 9–18 months	\$1.5M–\$4M	Not offered as prime today

The sprint 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. Every build in Section 9 exceeds the SAT, so the

agency competes it on its own terms; Avalon can perform that work as a subcontractor to a prime. The contracting officer decides whether the organizational conflict of interest rules in FAR subpart 9.5 limit the sprint vendor from competing for a build it scoped, and the sprint is worth buying either way, because the artifacts are vendor-neutral.

Avalon's rates sit at a \$165 to \$195 an hour anchor, inside the \$115 to \$225 market band, and the same rate table applies to any adjacent Avalon service in one proposal. Prices are fixed against a named service, a dated dependency schedule and a stated week count. There is no performance-based fee.

Illustration: Sizing One MVP by Its Integrations

The figures below are a planning illustration for one representative unclassified service. They are not a quote and not a result from any engagement. The build is modeled as a 4-week steel thread, 8 weeks of core features and 4 weeks for each named legacy integration (the knowledge base range is two to six), run in series by a 4.5 FTE team at \$165 to \$195 an hour.

Named integrations	Weeks	Months	Hours	Rate-band range	Inside \$450K–\$1.2M
2	20	4.6	3,600	\$594K–\$702K	Yes
4	28	6.5	5,040	\$832K–\$983K	Yes
6	36	8.3	6,480	\$1.07M–\$1.26M	No: mid-size

Two integrations fit the small-system profile in about 4.6 months. Four stay inside the price band but stretch past six months. Six take about 8.3 months and break the band at the top. Integration count moves the price more than feature count does, which is why the roadmap names each integration and prices the ones beyond the base scope as optional line items.

What Waiting Costs

Access delays burn paid time. At 4.5 FTE, a two-week wait for accounts costs the build \$59.4K to \$70.2K; an eight-week wait costs \$238K to \$281K. The sprint team is smaller, but an eight-week wait still costs more than the sprint itself. Dated government-furnished items in the statement of work turn that risk into a schedule term.

What the Sprint Costs

Scope	FTE	Hours	Rate-band range	Planning fee	Inside \$45K–\$85K
Short (3 weeks)	1.85	222	\$36.6K–\$43.3K	\$45K	Floor applies
Base (4 weeks)	1.85	296	\$48.8K–\$57.7K	\$53K	Yes
Long (6 weeks)	1.85	444	\$73.3K–\$86.6K	\$80K	No: cap scope
Long, public-facing (6 weeks + UX 0.25)	2.1	504	\$83.2K–\$98.3K	\$85K	No: cap scope

The base case is a four-week sprint: a cloud architect at 1.0 FTE, a DevSecOps engineer at 0.5, a delivery lead at 0.25 and a compliance liaison at 0.1. That is 296 hours, or \$48.8K to \$57.7K, with a \$53K planning fee at the midpoint. A three-week sprint drops to \$36.6K at the low end, under the \$45K floor, so the fee does not go below \$45K. A six-week sprint runs \$73.3K to \$86.6K, at the top of the band. Adding a quarter-time UX researcher for a public-facing service pushes it to \$98.3K, so the sprint either holds at six weeks without UX research or prices the research separately. Every case sits far below the simplified acquisition threshold.

Common Pitfalls

Pitfall	How to avoid it
Scope creep dressed as agility	Capacity-based scope, a written MVP, a done-definition in the QASP and change control for new epics
Integration sprawl	Cap integrations by name in the base scope; price the rest as optional line items
Agency access delay read as vendor failure	Dated government-furnished items in the statement of work
"MVP" heard as the full legacy feature set	A signed MVP scope statement from the sprint
Compliance oversell	Evidence for developer-owned controls; the AO decides
Inconsistent rates across bundled services	One rate table per proposal
Penetration testing your own build	Formal testing by an independent party under separate tasking
Accessibility left to the end	508 testing in every sprint

Conclusion and Next Step

A cloud native build fails or succeeds on decisions made before it starts: how many integrations, what the first release must do, which platform it runs on and how the ISSO will receive evidence. Those decisions cost tens of thousands of dollars to make well and hundreds of thousands to make late.

The natural first step is the fixed-fee discovery sprint: one mission service, two to four weeks, under the simplified acquisition threshold, ending in an integration inventory, a confirmed authorization pathway, a reference architecture, a signed MVP scope and a priced build roadmap the agency owns. To discuss a service, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

Cloud native

Software built for cloud platforms: containers or managed services, infrastructure as code and automated pipelines. A lifted-and-shifted monolith is cloud-hosted, not cloud native.

Steel thread

A minimal end-to-end slice of the application deployed through the full pipeline to a production-like environment.

MVP

Minimum viable product: production software behind real security gates, smaller in scope than the full system, not lower in quality.

Modular monolith

One deployable application with clear internal module boundaries; a valid cloud native answer for smaller systems.

Infrastructure as code

Environments defined in reviewable code, such as Terraform or OpenTofu, instead of configured by hand.

SBOM

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

Developer-owned controls

NIST SP 800-53 controls implemented in the application and pipeline, as opposed to those inherited from the platform or run by the agency.

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 service. None is drawn from a specific agency, a real system or a completed engagement.

Assumption	Value	Basis
Build schedule	4 weeks steel thread, 8 weeks core features, 4 weeks per integration, in series	Knowledge base ranges; planning assumption
Build team	Lead 1.0, engineers 2.0, DevSecOps 0.75, delivery lead 0.5, compliance 0.25	4.5 FTE
Sprint team	Architect 1.0, DevSecOps 0.5, delivery lead 0.25, compliance 0.1	1.85 FTE, four weeks
Rates	\$165–\$195 an hour, 40 hours a week	Category anchor inside the \$115–\$225 market band
Price checks	Sprint \$53K; two-integration build \$594K–\$702K	Inside \$45K–\$85K and \$450K–\$1.2M

Appendix C: References

1. **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>
2. **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>
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 800-190, Application Container Security Guide*
<https://csrc.nist.gov/pubs/sp/800/190/final>
5. **National Institute of Standards and Technology**, *SP 800-204, Security Strategies for Microservices-based Application Systems*
<https://csrc.nist.gov/pubs/sp/800/204/final>

6. **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>
7. **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>
8. **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>
9. **FedRAMP**, *FedRAMP program and 2026 Consolidated Rules*
<https://www.fedramp.gov>
10. **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>
11. **Department of Defense CIO**, *DoD Enterprise DevSecOps Reference Design and related documents*
<https://dodcio.defense.gov/library/>
12. **U.S. Access Board**, *Section 508 Information and Communication Technology standards*
<https://www.access-board.gov/ict/>
13. **U.S. Congress**, *21st Century Integrated Digital Experience Act, P.L. 115-336*
<https://www.congress.gov/bill/115th-congress/house-bill/5759>
14. **General Services Administration**, *U.S. Web Design System*
<https://designsystem.digital.gov>
15. **Microsoft**, *Product lifecycle search: SQL Server 2016 and Windows Server 2016*
<https://learn.microsoft.com/en-us/lifecycle/>
16. **Acquisition.gov**, *FAR 15.305, Proposal evaluation*
<https://www.acquisition.gov/far/15.305>

17. **Acquisition.gov**, *FAR subpart 9.5, Organizational and Consultant Conflicts of Interest*

<https://www.acquisition.gov/far/subpart-9.5>

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/>