



Securing Tomorrow's Missions Today.



Onboard Once, Inherit Correctly: Getting a Federal Program Productive Inside a Government Shared Cloud

Gov-Shared Cloud Services: platform fit, onboarding, and an inheritance map your assessor will accept.

Executive Summary	2
Why "Use the Enterprise Cloud" Is Harder Than It Sounds	3
The Myth That Causes the Most Trouble	3
What Triggers the Work	3
Choosing the Right Shared Environment	4
What the Engagement Delivers	6
Deliverables	7
What This Service Does Not Include	8
Control Inheritance: What the Platform Covers and What the Program Still Owns	8
How the Work Maps to Federal Frameworks	9
What Avalon Does and Does Not Certify	10
Connectivity and Identity Inside the Platform's Guardrails	10
How Delivery Works: A Fixed-Fee Onboarding Sprint	10
The Avalon Team	11
What the Agency Provides	11
Pricing, Contracting and the Cost of Going It Alone	12
An Illustrative Comparison: Build Your Own or Onboard	12
Sensitivity	14
Risk Register	15
Acquisition Pathways	16
Common Pitfalls and Questions Agencies Ask	17
Where Onboarding Leads Next	18
Conclusion and Next Step	18
Appendices	19
Appendix A: Glossary	19
Appendix B: Control Inheritance Example	20
Appendix C: Comparison Assumptions	21
Appendix D: References	22

Executive Summary

Most federal programs no longer choose whether to use the cloud. They are told which one. DoD components direct programs toward enterprise environments such as the Department of the Air Force's Cloud One and the Army's cArmy, and toward commercial cloud bought through the Joint Warfighting Cloud Capability (JWCC). Civilian agencies steer programs toward agency enterprise clouds, GSA's cloud.gov, and FedRAMP-certified shared offerings. These platforms exist so that a program office does not have to engineer and secure its own cloud.

Getting onto one is still real work. Someone has to pick the right platform for the program's data and impact level, get the funding document and intake forms through without losing a place in the queue, configure the program's tenant inside the platform's guardrails, connect identity and network paths, and write down which security controls the platform covers and which the program still owns. Most program offices do not have spare people for any of that.

This paper is written for the people who carry that problem: program managers and mission owners with a deadline, the component CIO or cloud program office that set the direction, the ISSM or ISSO who has to defend the authorization story, and the contracting officer who buys the help. It describes Avalon Technology Services' Gov-Shared Cloud Services:

- **Platform fit and selection.** A scored comparison of candidate shared environments and a decision record the program can defend.
- **Onboarding execution.** The platform's intake process driven end to end, including the funding document.
- **Tenant configuration.** Accounts, segmentation, connectivity, identity federation, logging and tagging, set up inside the platform's guardrails.
- **A Control Inheritance Workbook.** A control-by-control reconciliation against NIST SP 800-53 that the ISSO can lift directly into the System Security Plan.

The work is sold as a fixed-fee sprint of three to ten weeks, or as the first workstream of a larger migration. Section 8 compares two paths for a representative program. In that illustration, building a bespoke cloud environment costs \$1.01M more over three years than onboarding to the enterprise platform, before counting the 6 extra months the program waits to become productive.

Why "Use the Enterprise Cloud" Is Harder Than It Sounds

A directed move to a shared platform looks like a paperwork exercise from above. From inside the program office it carries four kinds of risk.

Risk	How it shows up
Mission	A system stuck on aging infrastructure, or waiting months in a platform onboarding queue, cannot deliver capability. Directed-migration deadlines slip and the program absorbs the blame.
Compliance	Mission owners often assume the platform's authorization covers them. It does not. The mission system still needs its own authorization, and inheritance that is not documented reads as unmet controls at assessment time.
Cost	Programs that bypass the shared environment and open their own cloud accounts pay twice: once for duplicate engineering, and again when an IG or cost review flags the duplication. Consumption billed through a platform with no tagging or chargeback model becomes spend nobody can see.
Operational	A tenant configured around the platform's guardrails instead of within them breaks at the next platform update. Identity and connectivity shortcuts turn into outages and findings later.

The Myth That Causes the Most Trouble

"The platform has an ATO, so we're covered" is the single most expensive misunderstanding in shared cloud. The platform's authorization covers the platform. Under the NIST Risk Management Framework, the mission system is still its own system with its own boundary, and its Authorizing Official still makes their own decision. What the platform offers is a set of controls the program can inherit, provided the program documents that inheritance control by control. FedRAMP makes the same distinction in its 2026 Consolidated Rules: it now calls a qualifying offering "FedRAMP Certified," while agencies still authorize their own use.

What Triggers the Work

- A directed-migration memo from the component CIO or cloud program office.

- A data center closure or lease expiration with a hard move-out date.
- A new-start system that needs an authorized environment before development can begin.
- A stalled or expiring ATO on a bespoke environment.
- A security incident or audit that exposed unmanaged cloud accounts.
- Fourth-quarter O&M funds that can pay for a short fixed-fee sprint.

The demand behind these triggers is growing. DISA reported more than \$3.9 billion in JWCC task orders by late 2025, with the Air Force onboarding and large Army orders the year before. Every new task order is a program that still has to get productive inside the environment it bought.

Choosing the Right Shared Environment

The first question is not how to onboard but where. The answer depends on the program's data, impact level and mission, not on which platform is most familiar. The fit assessment inventories the program's workloads and data types (CUI, PII, PHI and classification level) and scores each candidate environment against the same criteria.

Candidate environment	Typical fit
JWCC task orders (commercial cloud through DISA)	DoD programs buying AWS, Google, Microsoft or Oracle capacity directly
Department of the Air Force Cloud One	Air Force and Space Force programs; broader DoD use where supported
Army cArmy	Army programs directed to the enterprise environment
Department of the Navy environments	Navy and Marine Corps programs, including Flank Speed-adjacent work
DISA Stratus	DoD workloads suited to DISA's on-premises cloud
VA Enterprise Cloud	VA health and benefits systems
GSA cloud.gov	Civilian applications that fit a FedRAMP-authorized platform-as-a-service; small agencies without a cloud team
FedRAMP-certified shared SaaS and shared services	Commodity functions an agency should buy rather than host

Each candidate is scored on five criteria: support for the required impact level, the controls the program can inherit, the cost model, onboarding lead time, and exit terms. The result is a recommendation with a written decision record, so the program can defend the choice to its CIO, its assessor and its budget office. Sometimes the honest answer is that no shared environment fits, and the program needs its own architecture. The assessment says so.

What the Engagement Delivers

Activity block	What Avalon does
1. Platform fit and selection	Inventory workloads and data types, score candidate environments, and recommend a destination with a decision record.
2. Onboarding execution	Drive the platform's intake end to end: sponsor and funding coordination (MIPR or interagency agreement), account and enclave requests, impact-level determination support, region selection, and every intake form, submitted correctly the first time.
3. Tenant landing-zone configuration	Inside the platform's guardrails: account structure, segmentation, connectivity path, identity federation, logging hookup, tagging standard, and baseline infrastructure-as-code where the platform permits it.
4. Control inheritance mapping	Reconcile the platform's authorization against the mission system's NIST SP 800-53 control set: inherited, shared and program-owned, control by control.
5. Governance and handoff	Consumption and chargeback model, service-request runbook, roles and permissions, exit and portability notes, and a working-session handoff to program staff.

Deliverables

Deliverable	Format
Platform Fit and Selection Assessment, with scoring matrix and decision record	Report plus scoring workbook
Onboarding runbook and completed intake artifact set	Document plus copies of submitted platform artifacts
Configured tenant landing zone	Live configuration plus infrastructure-as-code repository where the platform allows customer-managed code
Control Inheritance Workbook	Spreadsheet mapped to NIST SP 800-53, structured for direct SSP import
Connectivity and identity integration design note	Diagram plus short design document
Governance, tagging and chargeback standard	Document plus tag dictionary
Handoff briefing	Slides plus a recorded working session

What This Service Does Not Include

Not included	Where it belongs instead
Migrating or refactoring the applications	Cloud Migration & Development; this service ends at a tenant-ready state against a written acceptance checklist
Designing a bespoke, agency-owned cloud	Cloud Architecture & Engineering, when the fit assessment concludes no shared environment fits
Writing the full SSP or running the ATO process	System Security Plans and ATO Process Facilitation; the workbook is an input to both
Steady-state operations and monitoring	Enterprise Monitoring or a separate O&M arrangement
Cloud consumption	Bought by the agency through the platform's vehicle; Avalon resells nothing and marks up nothing
Historical cost audit and recovery	FinOps

Control Inheritance: What the Platform Covers and What the Program Still Owns

Inheritance is where shared cloud either pays off or quietly fails. A platform's authorization lets a tenant inherit some controls completely, share others, and leaves the rest entirely with the program. The Customer Responsibility Matrix published with the platform's authorization says which is which in general terms. It does not say how those responsibilities apply to one specific mission system.

The Control Inheritance Workbook closes that gap. For every control in the mission system's baseline, it records whether the control is inherited, shared or program-owned, what evidence supports that position, and who on the program owns the remaining work. It is built for the ISSO, and it is formatted so rows can move directly into the System Security Plan.

Stated precisely: **this effort positions the program to inherit the maximum defensible set of controls from the platform's authorization and documents the remaining mission-owner responsibilities in an assessor-ready Customer Responsibility Matrix reconciliation.**

How the Work Maps to Federal Frameworks

Framework	What this service addresses
NIST SP 800-53 Rev. 5 and RMF (SP 800-37)	Control-by-control reconciliation across families such as AC, AU, CA, CM, IR, SC and SI. Speeds the RMF Prepare, Categorize, Select and Implement steps by using the platform as a common control provider. The Authorize step remains the AO's.
FedRAMP	Verifies the destination offering's certification status and class, and documents the agency's use of it. FedRAMP's 2026 Consolidated Rules use "FedRAMP Certified" with classes A through D.
DoD Cloud Computing SRG	Impact-level determination support and verification that the destination holds a DISA provisional authorization at the required level.
FISMA	Defines the mission system's boundary inside the shared environment, a frequent point of assessor confusion.
DoD Secure Cloud Computing Architecture (SCCA)	Connectivity through Cloud Access Points and SCCA components, so the tenant's network path is compliant by construction.
DoD Zero Trust Strategy	Maps which zero trust activities the platform delivers and which the tenant must implement ahead of the FY2027 target-level deadline.
TIC 3.0 (civilian)	Aligns the tenant's connectivity to the applicable CISA TIC 3.0 use case.
ICAM (OMB M-19-17) and HSPD-12	CAC and PIV-based identity federation into the tenant.

What Avalon Does and Does Not Certify

Avalon does not issue Authorizations to Operate, DISA provisional authorizations or FedRAMP certifications, and does not guarantee any authorization outcome or timeline. Platform authorizations belong to the platform's authorizing officials, and the mission system's authorization rests with the agency's AO. The onboarding, configuration and inheritance work is readiness and advisory work: it makes the authorization achievable and defensible, and it is not the authorization itself.

Connectivity and Identity Inside the Platform's Guardrails

Every shared platform publishes guardrails: the account structures, network patterns, identity providers and logging paths its tenants must use. Tenant configuration works within those guardrails. Configuration that works around them may go live faster, but it breaks at the next platform update and damages the program's relationship with the platform office.

- **Connectivity.** For DoD tenants, the network path runs through Cloud Access Points and SCCA components. For civilian tenants, it is aligned to the applicable TIC 3.0 use case.
- **Identity.** CAC or PIV-based federation through the agency's ICAM service or an authorized identity provider, with role-based access defined for the program's staff and contractors.
- **Segmentation.** Network segmentation inside the mission enclave, so the program's workloads are separated from other tenants and from each other where required.
- **Logging.** Tenant logs connected to the platform or agency security operations center, so monitoring is continuous from the first day.
- **Tagging.** A tag dictionary applied from the start, so consumption billed through the platform can be attributed, charged back and reviewed.
- **Infrastructure-as-code.** Baseline configuration in Terraform or OpenTofu using DoD Cloud IaC baselines or platform-provided modules, where the platform allows customer-managed code, written so the program's own staff can maintain it.

How Delivery Works: A Fixed-Fee Onboarding Sprint

Sold on its own, the service is a three-to-six week fit assessment and onboarding sprint. Tenant configuration and the inheritance workbook add time when the destination is

already decided, for a total of four to ten weeks. Inside a Cloud Migration & Development engagement, it is the first two-to-six week workstream, completed before any workload moves.

Duration depends on impact level and the number of enclaves far more than on the size of the agency. An IL5 enclave with SCCA connectivity work takes weeks longer than an IL2 tenant or a civilian FedRAMP Moderate tenant.

The Avalon Team

Role	Involvement
Cloud solutions architect (founder-level)	Leads delivery at 50–75%
Cloud and platform engineer	About 50%
Compliance specialist	About 25%, focused on the inheritance workbook

What the Agency Provides

Platform queue time is the one schedule driver Avalon does not control. Every agency- and platform-dependent step goes into the statement of work with a date and an owner, with schedule relief tied to those dates:

- A named mission-owner sponsor.
- A funding point of contact authorized to execute the MIPR or interagency agreement.
- ISSM or ISSO availability of two to four hours a week.
- A network point of contact who can action change requests.
- An accurate system and data inventory at kickoff.
- Prompt action on platform intake steps.

Pricing, Contracting and the Cost of Going It Alone

Offering	Typical price (firm fixed price)	Duration
Shared cloud fit assessment and onboarding roadmap	\$25K–\$75K	3–6 weeks
Onboarding execution, tenant configuration and inheritance workbook	\$60K–\$175K	4–10 weeks
Inside a Cloud Migration & Development engagement	A fixed line item, typically 10–20% of the migration's services value	First 2–6 weeks

These are market-norm planning ranges, validated against the specific program before any figure appears in a proposal.

Firm fixed price is the default because the work is bounded and deliverable-defined. When integration unknowns are high, such as an unusual identity architecture or a contested connectivity path, a small time-and-materials allowance can cover the configuration block while the rest stays fixed. Cost goes up with IL5 scope and SCCA connectivity, multiple enclaves or cloud providers, and cleared-staff requirements. It goes down for IL2 or civilian FedRAMP Moderate destinations and when the destination is already decided.

GSA's OneGov agreements have put cloud credits in agency hands. The AWS agreement, for example, offers up to \$1 billion in incentive credits across civilian agencies through December 31, 2028. These credits generally fund consumption and provider-delivered support, not independent tenant-side work, but onboarding correctly is how a program actually uses them.

An Illustrative Comparison: Build Your Own or Onboard

This is an illustration, not a quote and not a result. It compares two paths for one representative unclassified program over three years. Cloud consumption is the same in both paths and is left out. Every input is listed in Appendix C.

Cost line	Build your own environment	Onboard to the enterprise platform
One-time engineering and setup	\$420K	\$165K (Avalon fixed fee)
One-time authorization work	\$350K (no inherited controls)	\$150K (program-owned controls only)
Annual operations staff	\$330K (2 FTE)	\$165K (1 FTE)
Annual continuous monitoring	\$120K	\$50K
Annual contract or platform fees	\$40K (separate cloud contract)	\$90K (platform service fee)
Year 1 total	\$1.26M	\$620K
Three-year total	\$2.24M	\$1.23M
Months until productive	9	3

What the comparison shows

- **Three-year difference:** onboarding costs \$1.01M less, or \$999K in present value discounted at 1.1%, the three-year real rate in OMB Circular A-94 Appendix C for 2026.
- **Year 1 difference:** \$640K, mostly because the program does not engineer an environment or carry a full authorization package alone.
- **Time to productive:** 6 months sooner. At \$120K a month in program staff and contractor time spent waiting or reworking, that is another \$720K not counted in the totals above.

Sensitivity

Scenario	Year 1 difference	3-year difference	Time saved (value)
Base case	\$640K	\$1.01M	6 months (\$720K)
Platform service fee doubles (\$180K a year)	\$550K	\$740K	6 months (\$720K)
Weaker inheritance (program-owned work \$250K; monitoring \$90K a year)	\$500K	\$790K	6 months (\$720K)
Platform queue adds 3 months (6 months to productive)	\$640K	\$1.01M	3 months (\$360K)
Building your own costs 30% less	\$409K	\$779K	6 months (\$720K)

Onboarding stays cheaper in every scenario tested, but the size of the advantage depends on how much the platform really lets the program inherit and what the platform charges tenants. Both are measured during the fit assessment for the actual candidate platforms. When no shared environment supports the program's impact level or mission, the comparison does not apply, and the assessment says so.

Risk Register

ID	Risk	Likelihood	Impact	Mitigation built into the plan
R-1	Platform intake queue or funding document stalls the schedule	High	High	Every agency and platform step dated in the SOW with an owner; schedule relief tied to those dates
R-2	Scope drifts into migrating the applications	Medium	High	End state defined as a tenant-ready environment against a written checklist; migration priced separately
R-3	Inheritance claimed but not documented	Medium	High	Control-by-control workbook with evidence references, reviewed with the ISSO before handoff
R-4	Configuration conflicts with platform guardrails	Medium	Medium	Configuration built from platform-provided modules and reviewed against published guardrails
R-5	Identity federation or connectivity approval takes longer than planned	Medium	Medium	Design note agreed with the network and identity owners in week one; small T&M allowance where unknowns are high
R-6	No one owns the environment after handoff	Medium	Medium	Roles, runbook and handoff session in the base scope; operations owner named at kickoff

Acquisition Pathways

Vehicle	Fit for this service	Avalon's access
GSA Multiple Award Schedule, SIN 518210C	The natural home for a standalone sprint; agencies can issue a small fixed-price order quickly	Avalon's priority vehicle
NASA SEWP VI	Contract period starts November 1, 2026; Categories B and C cover services, and all categories support small business set-asides	Near term, as a subcontractor to Category B or C holders
GSA Alliant 3	Large modernization task orders where this service is one line item	Subcontractor to awardees
OASIS+	Services orders where the parent engagement is broader modernization	On-ramp candidate
JWCC	Compute is bought from the cloud providers; tenant-side help is bought separately	Market context, not a contracting path
Agency and component BPAs, small business set-asides	The sprint is sized as a BPA call	Direct

Onboarding existing systems is usually funded with one-year O&M money, which is why demand peaks in the fourth quarter. Programs tend to plan the buy between April and June and need it awardable in days between July and September. A fixed-fee sprint with defined deliverables is a clean fit for that window. A system still in development may fund the same work with RDT&E.

Common Pitfalls and Questions Agencies Ask

Pitfall	How the plan prevents it
"While you're in there, migrate the app"	The SOW defines the end state as a tenant-ready environment and says that workload migration is separately scoped
"Also fix our rogue accounts"	Remediating environments built outside the platform is priced as an option, never absorbed
Compliance oversell	No claim that the platform's ATO covers the program, that an impact-level decision is an authorization milestone, or that the workbook is the SSP
Agency-side delays read as vendor failure	Every dependent step is dated in the SOW, with schedule relief when those dates slip
Code the program cannot maintain	Infrastructure-as-code built on platform modules and handed off in a working session
No exit plan	Exit and portability notes in the base scope, for the platform's next recompute

- **"The platform team onboards us for free."** The platform office onboards at portfolio scale: forms, an account, documentation. The program-specific work, including your identity federation, your network path and your inheritance documentation, is what the intake queue does not provide.
- **"The platform already has an ATO. Why pay for compliance work?"** The platform's authorization covers the platform. Your system still needs its own, and every inherited control must be documented or the assessor treats it as unmet.
- **"Why not task the integrator already running the platform?"** Platform operators work for the platform office at enterprise scale. A tenant-side firm works only for the program, and there is no conflict of interest in advising one tenant.
- **"Can't we just open our own accounts faster?"** You can, and Section 8 shows what it usually costs. Programs that do often meet the issue again in an IG finding or a cost review.

Where Onboarding Leads Next

Next step	Why it follows onboarding
Cloud Migration & Development	The tenant is ready; the applications still have to move
System Security Plans and ATO Process Facilitation	The inheritance workbook feeds the SSP and the assessment directly
FinOps	The tagging and chargeback standard makes cost governance possible
Enterprise Monitoring	Someone has to run and watch the environment after handoff
Zero Trust Architecture	The platform-versus-tenant zero trust map becomes the program's implementation plan

Several dates shape the demand. SEWP VI opens for orders on November 1, 2026. The AWS OneGov credits run through December 31, 2028. DoD's target-level zero trust deadline falls at the end of FY2027. DISA has been preparing a follow-on to JWCC. Each of these pushes more programs into shared environments that they will need help onboarding onto.

Conclusion and Next Step

Shared cloud platforms remove the need for every program to build its own cloud. They do not remove the need to get onto them correctly. A program that picks the right platform, onboards without rework, configures within the guardrails and documents its inheritance control by control reaches a productive, defensible environment months sooner, and walks into its assessment with evidence instead of assumptions.

The first step is a fixed-fee shared cloud fit assessment. It scores the candidate platforms against the program's data and impact level, prices both paths, and lays out a dated onboarding plan. Avalon takes on one onboarding engagement at a time, at unclassified scope (IL2, IL4 or civilian FedRAMP Moderate), with founder-level attention on the work. To discuss an assessment, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

ATO: Authority to Operate

The Authorizing Official's formal decision to accept the risk of operating a system under the NIST Risk Management Framework.

Cloud Access Point (CAP)

The DoD-approved boundary through which DoD networks connect to commercial cloud at IL4 and IL5.

Control inheritance

Using a security control implemented by a common control provider, such as a shared platform, in place of implementing it within the program's own system.

CRM: Customer Responsibility Matrix

The document published with a platform's authorization that states which control responsibilities fall to the platform and which to its customers.

FedRAMP

The federal program that standardizes security assessment of cloud offerings. Under its 2026 Consolidated Rules it certifies offerings in classes A through D; agencies still authorize their own use.

ICAM: Identity, Credential and Access Management

The policies and services that manage digital identities and access, governed for federal agencies by OMB M-19-17.

IL: Impact Level

DoD's categories for cloud data sensitivity under the Cloud Computing SRG: IL2, IL4, IL5 and IL6.

JWCC: Joint Warfighting Cloud Capability

DoD's multi-award contract for commercial cloud from AWS, Google, Microsoft and Oracle, managed by DISA.

MIPR: Military Interdepartmental Purchase Request

The funding document used to transfer funds between DoD organizations, often required for platform onboarding.

SCCA: Secure Cloud Computing Architecture

DoD's reference architecture for connecting to and protecting workloads in commercial cloud.

SSP: System Security Plan

The document describing a system's boundary, environment and how each security control is implemented.

TIC 3.0: Trusted Internet Connections

CISA's program for securing federal civilian network traffic, organized into use cases.

Appendix B: Control Inheritance Example

A simplified example of how the Control Inheritance Workbook classifies controls for a tenant on a shared IaaS platform. Actual classifications depend on the platform's authorization and customer responsibility matrix.

Control	Typical position	What the program still documents or does
PE-3 Physical Access Control	Inherited	Reference the platform's authorization; no program action
AC-2 Account Management	Shared	Program accounts and roles, reviews, and federation to the agency identity provider
AU-6 Audit Record Review	Shared	Review of tenant logs; platform provides collection and storage
CM-6 Configuration Settings	Shared	Settings for the program's workloads within platform baselines
IA-2 Identification and Authentication	Shared	CAC or PIV federation for program users
SC-7 Boundary Protection	Shared	Tenant segmentation and allowed flows; platform provides the perimeter and CAP or TIC path
IR-4 Incident Handling	Shared	Program incident procedures and handoffs to the platform's security operations
SI-2 Flaw Remediation	Program-owned	Patching of the program's operating systems and applications

Control	Typical position	What the program still documents or does
CA-2 Control Assessments	Program-owned	Assessment of the mission system by its assessors

Appendix C: Comparison Assumptions

All values are Avalon planning assumptions for one representative unclassified program, in constant FY2026 dollars. None is drawn from a specific agency or a completed engagement.

Category	Assumption	Value
Build your own (one-time)	Environment engineering (accounts, network, security baseline, connectivity)	\$420K
Build your own (one-time)	Full authorization package with no inherited controls (SSP, assessment prep, independent assessment)	\$350K
Build your own (annual)	Environment sustainment and security operations (2 FTE)	\$330K
Build your own (annual)	Continuous monitoring across the full control set	\$120K
Build your own (annual)	Separate cloud contract administration	\$40K
Onboard (one-time)	Avalon fit assessment (FFP)	\$45K
Onboard (one-time)	Avalon onboarding, tenant configuration and inheritance workbook (FFP)	\$120K
Onboard (one-time)	Authorization work for program-owned controls only	\$150K
Onboard (annual)	Tenant operations (1 FTE)	\$165K

Category	Assumption	Value
Onboard (annual)	Continuous monitoring of program-owned controls	\$50K
Onboard (annual)	Platform service fee	\$90K
Timing	Months until the program has a usable environment ready for authorization	9 (build) vs 3 (onboard)
Delay cost	Program staff and contractor time spent waiting or reworking, per month	\$120K
Labor rate	Fully loaded cost per FTE	\$165K
Discount rate	OMB Circular A-94 Appendix C, 3-year real rate for 2026, mid-year convention	1.1%
Excluded	Cloud consumption (the same in both paths); inflation	-

Appendix D: References

1. **FedRAMP**, *FedRAMP Consolidated Rules for 2026: Definitions*
<https://www.fedramp.gov/2026/definitions/>
2. **MeriTalk**, *DISA Reports Growth in JWCC Cloud Orders, December 11, 2025*
<https://www.meritalk.com/articles/disa-reports-growth-in-jwcc-cloud-orders/>
3. **Oracle**, *U.S. Department of the Air Force Accelerates Cloud Modernization with Oracle, February 12, 2026*
<https://www.oracle.com/news/announcement/us-department-of-the-air-force-accelerates-cloud-modernization-with-oracle-2026-02-12/>
4. **U.S. General Services Administration**, *GSA Announces OneGov Agreement with AWS, August 7, 2025*
<https://www.gsa.gov/about-us/newsroom/news-releases/gsa-announces-onegov-agreement-with-aws-08072025>
5. **NASA SEWP**, *SEWP VI Transition Updates*
https://www.sewp.nasa.gov/sewpv/sewpvi_transition_updates.shtml

6. **Office of Management and Budget**, *Circular A-94, Appendix C: Discount Rates for Cost-Effectiveness Analysis (2026)*
<https://www.whitehouse.gov/wp-content/uploads/2026/03/CircularA-94Appendix-C.pdf>
7. **Office of Management and Budget**, *M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management (May 2019)*
<https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf>
8. **Cybersecurity and Infrastructure Security Agency**, *Trusted Internet Connections (TIC) 3.0*
<https://www.cisa.gov/resources-tools/programs/trusted-internet-connections-tic>
9. **U.S. Department of Defense**, *DoD Zero Trust Strategy (November 2022)*
<https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf>
10. **DISA**, *Department of Defense Cloud Computing Security Requirements Guide*
<https://public.cyber.mil/dccs/>
11. **NIST**, *SP 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations*
<https://csrc.nist.gov/pubs/sp/800/37/r2/final>
12. **NIST**, *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>