



Securing Tomorrow's Missions Today.



Licensed Is Not Integrated: Phishing-Resistant MFA and Automated Deprovisioning for Component and Bureau ICAM

Identity & Access Management (IAM) Integration: the identity platform you already own, wired to your applications, your PIV/CAC credentials and your HR source.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
Licensed Is Not Integrated	3
Why It Concentrates in Government	3
How the Need Sounds	4
The Mandate Calendar	5
What the Service Does	6
Legacy Applications Make It Methodical, Not Impossible	7
PIV at the Desktop Is Not MFA at the Application	7
Evidence Assessors Can Use	8
How an Engagement Runs	10
Deliverables	11
What the Agency Provides	11
What Is Not Included	12
How Avalon Staffs It	12
Pricing and How to Buy	13
Illustration: Per-Application Wave Pricing	14
Common Pitfalls	16
Conclusion and Next Step	16
Appendices	17
Appendix A: Glossary	17
Appendix B: Illustration Assumptions	18
Appendix C: References	18

Executive Summary

Most federal components already own an identity platform. Microsoft Entra ID, Okta for Government or Ping sits in the license inventory, PIV or CAC cards unlock the desktop, and the zero trust implementation plan says "enterprise identity" on the first page. Yet the same component often has applications with their own local logins, a deprovisioning process that runs on tickets and email, and an access-recertification finding that comes back every audit cycle.

That gap between owning the platform and enforcing it at every application is where identity work actually happens. Licensing an identity provider earns no credit on the identity pillar of a zero trust maturity score. Integrated applications, phishing-resistant multifactor authentication at each of them, and accounts that disappear automatically when people leave do.

This paper is written for the CISO or Deputy CIO who funds the work, the zero trust or ICAM program manager who champions it, the ISSM and ISSO who carry the findings, and the contracting officer and COR who buy it. It describes Avalon Technology Services' Identity & Access Management (IAM) Integration service: integrating the agency's own licensed identity provider with its applications, its PIV/CAC credentials and its authoritative HR source, at component or bureau scale.

- **An ICAM readiness assessment.** A fixed-price engagement of four to eight weeks that inventories identity stores and applications, finds orphaned and stale accounts, rates each application's integration readiness, and produces a target architecture and wave plan. In the illustration it is \$55K, bought open-market under the \$350,000 simplified acquisition threshold.
- **An integration program priced per application.** Foundation build, onboarding waves and closeout, with a published unit price for each application. A component program of this size exceeds the simplified acquisition threshold, so it is bought through a prime contractor, with Avalon as a subcontractor.

Section 9 works through an illustrative program for 30 applications: \$527K for foundation, 4 waves and closeout, about 6.9 months once the assessment is done, and what a higher legacy share, late application owners or a larger portfolio do to that plan.

The service implements controls and produces evidence. It does not assess those controls or grant an authorization: those belong to the agency's security control assessor and Authorizing Official.

Licensed Is Not Integrated

Risk	How it shows up
Mission	Every application with its own local accounts is a door that the identity provider does not see. Credential theft remains a leading way into federal systems, and an unmonitored login page is where it lands.
Compliance	Orphaned accounts, excessive privileges, missing MFA on older systems and access recertifications that exist only on paper are recurring FISMA, IG and A-123 findings. They land on the ISSM as POA&M items.
Separation	A separated employee's account found active months later. When deprovisioning depends on someone remembering to file a ticket for each system, this is an expected result, not an anomaly.
Cost	Manual account administration and paper access forms consume help-desk and ISSO hours, and duplicate point tools accumulate license spend.

Why It Concentrates in Government

- **Long-lived applications.** Agency portfolios span decades. Older applications were built around local accounts, Kerberos or header-based authentication and cannot consume a modern federated login directly, so MFA requirements stall at exactly the systems that matter most.
- **An existing credential program.** PIV and CAC under HSPD-12 and FIPS 201 mean integration is never greenfield. A new identity platform has to work with the existing certificate infrastructure, derived credentials and, for people who cannot use a card, FIDO2 security keys or passkeys.
- **Dated mandates.** OMB M-22-09 made enterprise identity and phishing-resistant MFA government-wide requirements, and the DoD Zero Trust Strategy makes the User pillar the foundation of its target-level activities. Those dates arrive faster than agency engineering staff can absorb them.

- **Workforce change wearing an IT badge.** New login flows, MFA enrollment and changed access requests need communications and training the agency co-owns. Treating identity as a pure configuration task is how pilots stall.

How the Need Sounds

"Deprovisioning is a manual ticket and it takes weeks." "Every app has its own login."
"We can't put PIV on that system, it's too old." "The IG dinged us on access recertification again." "We don't actually know how many service accounts we have."
Any two of these describe this service.

The Mandate Calendar

Date	Event	What it means for identity
January 26, 2022	OMB M-22-09, the Federal Zero Trust Strategy	Civilian agencies: enterprise-managed identities and phishing-resistant MFA for staff, contractors and partners
2023	CISA Zero Trust Maturity Model 2.0	A scored identity pillar (Traditional, Initial, Advanced, Optimal) usable as a before-and-after measure
September 24, 2025	DoD announces the Cybersecurity Risk Management Construct (CSRMC)	RMF, DoDI 8510.01 and eMASS remain in use; identity evidence still feeds the authorization record
May 2026	OMB M-26-14 replaced M-21-31	A risk-based logging model; identity events are among the logs that matter most
June 25, 2026	FedRAMP Consolidated Rules	Cloud identity products are "FedRAMP Certified" in classes A to D; certification covers the provider's offering, and the agency still authorizes its own system
June 11, 2027 / December 31, 2028	FedRAMP Rev5 transition	New Rev5 submissions stop, then Rev5 authorizations end; confirm the status of each identity product the agency relies on
September 30, 2027	End of FY2027	DoD components are due to reach target-level zero trust, with the User pillar as the foundation

DoD is also replacing the paper DD Form 2875 access request with automated ICAM workflows. For a DoD component, the useful question is not whether a milestone was announced but whether the automation is actually live for its applications. Automated joiner, mover and leaver processing is the work that makes it live.

What the Service Does

The service integrates what the agency already licenses. It does not resell software or host an identity platform; licenses stay with the agency's reseller, which keeps the advice neutral.

Workstream	Activities
Discovery and account hygiene	Inventory of identity stores (Active Directory, LDAP, cloud directories, application-local account tables) and non-person entities; reconciliation that finds orphaned, duplicate and stale accounts before anything moves
Identity provider hardening	Deploy or harden the IdP (Entra ID in GCC, GCC High or DoD tenants, Okta for Government, Ping or ForgeRock); conditional access and authentication policy design
Phishing-resistant MFA	PIV/CAC certificate authentication as primary; FIDO2 security keys or passkeys as the sanctioned alternative; SMS and voice one-time codes removed from policy
Application onboarding waves	SAML 2.0 or OpenID Connect integration; SCIM or connector provisioning where supported; a written legacy strategy for each application that cannot federate
Joiner, mover, leaver (JML)	The authoritative HR or personnel source connected to the identity system, so creation, role changes and deprovisioning happen automatically against an agreed service level
Access governance foundations	Role and attribute model (RBAC/ABAC), access request and approval workflows, certification campaigns in a governance tool the agency licenses
Bounded privileged access	Vaulting and session brokering for a capped list of privileged accounts where PAM tooling exists
Federation	Trusts with partner agencies, DoD enterprise ICAM services, or Login.gov for public-facing use

Legacy Applications Make It Methodical, Not Impossible

Some applications cannot federate natively. Each one gets one of three written patterns: an access gateway that authenticates the user and passes identity by header injection; Kerberos constrained delegation for Windows-integrated applications; or a documented risk acceptance with compensating controls that the agency decides on. The runbook states which mechanism protects the application, so the ISSO never discovers during assessment that a gateway-protected application was described as natively MFA-enforced. The mistake to avoid is letting the hardest tenth of the portfolio freeze the easy nine-tenths.

PIV at the Desktop Is Not MFA at the Application

A smart card at Windows login does not mean a phishing-resistant factor is enforced at each application behind it. Per-application enforcement is both the requirement and the gap, and it is what the identity pillar of a maturity assessment measures.

Evidence Assessors Can Use

Control (NIST SP 800-53 Rev. 5)	Evidence the service produces
IA-2, IA-2(1), IA-2(2), IA-2(12)	Authentication policy exports, MFA enforcement per application, PIV acceptance configuration
IA-4, IA-5	Identifier and authenticator management settings; removal of weak factors
IA-8	Federation trusts and non-organizational user configuration
IA-11, IA-12	Re-authentication rules; identity proofing linkage to the authoritative source
AC-2	JML automation configuration, deprovisioning service level, account reconciliation records
AC-3, AC-5, AC-6	Role and attribute model, separation-of-duty rules, privileged account register
AC-17	Conditional access rules for remote access
AU family (support)	Identity-event log forwarding to the agency's SIEM

Where the system handles controlled unclassified information under NIST SP 800-171, the same evidence maps to the 3.1 Access Control and 3.5 Identification and Authentication families. Evidence is delivered as a matrix plus artifacts, formatted for the system security plan and POA&M, and feeds the Implement and Assess steps of the RMF (SP 800-37 Rev. 2). The security control assessor draws the conclusions and the Authorizing Official makes the decision.

Accurate	Not accurate
Implements phishing-resistant MFA and automated account lifecycle management aligned to IA-2 and AC-2, with evidence for the authorization record and related POA&M items, subject to independent assessment	Achieves compliance, or delivers the ATO
Advances the identity pillar of the agency's zero trust plan	Makes the agency M-22-09 compliant, or delivers zero trust
Legacy application protected by a gateway with a documented compensating control	MFA compliant

How an Engagement Runs

Phase	Typical duration	What happens
Discovery	2–4 weeks	Access provisioning, stakeholder interviews, identity-store and application inventory, account-hygiene analysis, review of the SSP, POA&M and prior findings
Architecture and roadmap	2–4 weeks	FICAM-aligned target design, assurance-level selection under the NIST digital identity guidelines (SP 800-63), wave sequencing, success measures agreed with the ISSM
Foundation build	4–8 weeks	IdP hardening, PIV/CAC and FIDO2 policy, conditional access baseline, directory cleanup, federation trusts, JML connector
Onboarding waves	6–20+ weeks	A pilot wave of two or three representative applications, then waves of 5 to 15; legacy patterns; per-app runbooks and evidence
Transition and closeout	2–4 weeks	Knowledge transfer, admin training, O&M runbook, final evidence package, closeout brief mapping work to POA&M items

Discovery and architecture together are the readiness assessment. Its deliverables belong to the government and can be handed to any integrator, which also answers the organizational conflict of interest question: Avalon discloses and structures any follow-on under FAR subpart 9.5.

Deliverables

Deliverable	Format
Identity and Access Current-State Assessment	PDF report and spreadsheet inventory
Target Identity Architecture and Integration Roadmap	PDF and editable Visio or Draw.io source
Configured identity platform	Live configuration and as-built document
Application integration runbooks, one per app	Markdown or PDF in the agency's repository
JML workflow implementation	Live configuration and process document
Control-implementation evidence package (IA and AC)	Evidence matrix and artifacts for SSP and POA&M
Knowledge transfer and O&M runbook, admin training	Live sessions and written materials

What the Agency Provides

- Accounts and access for the delivery team, including CAC or PIV sponsorship and VPN. This is often the longest lead item (two to six weeks at DoD components), so the paperwork starts at award and the schedule starts when access is granted.
- A directory or platform administrator reachable at least part-time.
- An application owner for each application in a wave, at roughly 8 hours per application (4 to 12 is typical) for claims mapping, testing and cutover sign-off.
- Change-board access and reasonable change windows, plus test accounts and environments.
- The SSP, network diagrams and prior audit findings.

- A named application list as a contract appendix. Wave schedules re-baseline day for day when a dependency arrives late, and that rule is written into the statement of work.

What Is Not Included

Included	Separate work
Integrating applications to the IdP	Rewriting or refactoring application code
Configuring MFA and credential policy	Issuing PIV or CAC credentials (the agency's credentialing office or USAccess)
Evidence for IA and AC controls	Writing the full SSP, control assessment, the ATO
Bounded PAM onboarding with a capped account list	A full PAM program build, or SOC monitoring of identity events
Hygiene on existing directories	Directory consolidation or forest migration as its own program
Advice on licensed identity tooling	Software license resale
Physical access interface advice	PACS implementation

How Avalon Staffs It

Avalon takes one integration engagement at a time, in unclassified environments, with the readiness assessment runnable alongside it. Avalon has no past federal engagements under this service, and it cites no credential, clearance or partner status that is not current and verifiable. Avalon is not a delivery partner of any identity vendor and has no hosted identity product; it integrates the platform the agency already owns.

The assessment is led by an ICAM architect. Integration programs are delivered with IAM engineers named in the proposal, hired or subcontracted, and naming them is a condition of the offer rather than a promise made after award.

Requirement	How it is handled
Platform depth	Named personnel whose platform certifications (for example Entra or Okta) match the agency's stack, listed in the proposal
Senior security credential	A named lead whose security certification matches the agency's requirement, listed in the proposal
DoD privileged access	Personnel qualified under DoD 8140 for the work role, as a condition of the engagement
Investigation level	Investigation or clearance at the level the agency requires, as a condition of the engagement
Governance and PAM depth	Scoped conservatively; deeper IGA role engineering or PAM builds are teamed or quoted separately

Pricing and How to Buy

Shape	Market-norm range
ICAM readiness assessment and roadmap (4–8 weeks)	\$45K–\$95K fixed price
Foundation engagement (IdP hardening, MFA, pilot apps, small bureau, 3–5 months)	\$150K–\$400K
Component program (JML plus 20–50 apps in waves, 5–9 months)	\$400K–\$1.5M
Per-application unit (modern at the low end, legacy gateway at the high end)	\$8K–\$25K per app
Post-integration O&M	\$8K–\$30K a month
Blended labor	\$145–\$260 an hour

Evidence work is priced inside the engagement, not as a separate line. Per-application pricing turns an open-ended integration into countable units: the agency sees the price of each application before it is onboarded, and an added application is a priced modification rather than absorbed labor.

Only the assessment, and any other scope under the \$350,000 simplified acquisition threshold, is bought directly. That includes the readiness assessment and a small-bureau foundation engagement priced under the threshold, as open-market purchases with one-year O&M funds. Purchases between the \$15,000 micro-purchase threshold and the threshold are generally set aside for small business when two or more capable small businesses are expected to compete. A component integration program above the threshold is bought through a prime contractor that holds a suitable vehicle, with Avalon as a subcontractor. A program is never split into pieces to stay under the threshold. Avalon does not hold a GSA Schedule or a governmentwide contract today.

Identity work is mostly O&M-funded, which gives two buying windows: new-start funding from October to January for planned programs, and the July to September year-end period, when a fixed-price assessment fits.

Illustration: Per-Application Wave Pricing

The figures below are a planning illustration for one component, not a quote and not a result from any engagement. All inputs are assumptions listed in Appendix B.

The component has 30 applications on one identity provider. 6 of them (20%) are legacy applications that need a gateway, delegation or documented risk acceptance; the other 24 support SAML or OpenID Connect. A pilot wave of 3 applications is followed by waves of about 9. Two IAM engineers provide about 72 wave hours a week, and each wave's five-day cutover window overlaps the next wave's build.

Line	Basis	Price
Readiness assessment (bought first)	6 weeks, about 240 hours	\$55K
Foundation build	IdP hardening, MFA policy, hygiene, JML connector	\$160K
Modern applications	24 at \$8K	\$192K
Legacy applications	6 at \$25K	\$150K
Transition and closeout	Training, O&M runbook, final evidence	\$25K
Integration program (via a prime)	Foundation, waves, closeout	\$527K

The cross-check: at an assumed 32 engineering hours per modern application and 100 per legacy application, the unit prices imply about \$250 an hour, inside the \$145 to \$260 band. The assessment implies about \$229 an hour. The program total of \$527K sits inside the \$400K to \$1.5M component band. The agency's side is about 240 application-owner hours across the portfolio.

Scenario	Waves	Wave weeks	Program price	Months after assessment
Base case (30 apps, 20% legacy)	4	21	\$527K	6.9
Legacy share doubles (40%)	4	28	\$629K	8.5
App owners late (2 weeks slip per wave)	4	29	\$527K	8.8
Larger portfolio (40 apps)	6	30	\$641K	9.0

If the legacy share doubles to 40%, the price rises to \$629K and waves take 28 weeks instead of 21. The assessment is where that share is measured, which is why the program is priced after it rather than before. If application owners are two weeks late for

each wave, the price does not change but the program runs 8.8 months instead of 6.9; that slip is a documented, no-fault re-baseline, not a dispute. A 40-application portfolio adds 2 waves and reaches \$641K.

After closeout, an O&M retainer, illustrated at \$12K a month, administers the platform and onboards new applications at the same unit price.

Common Pitfalls

Pitfall	How to avoid it
"Just add these apps"	A named application list in the contract and a per-app price for additions
Directory cleanup turns into directory migration	Hygiene on existing directories only; consolidation is quoted separately
Bounded PAM drifts into a PAM program	A capped privileged-account count in the contract
The integrator becomes the help desk	A five-business-day cutover support window per wave, then O&M or the agency
Schedule starts at award, not at access	Access as a dated government milestone, reported from week one
Overstating a gateway-protected app	Each runbook states the actual mechanism and any compensating control

Conclusion and Next Step

Identity is the pillar every other zero trust investment depends on, and most of the remaining work is not buying software. It is the methodical integration of applications one at a time, the removal of weak factors, and a leaver process that does not depend on anyone remembering a ticket. Done well, it leaves evidence an assessor can verify and a runbook the next administrator can follow.

The natural first step is the ICAM readiness assessment: a fixed price under the simplified acquisition threshold, an inventory of every identity store and application, an account-hygiene finding list, and a per-application wave plan that prices the integration

before anyone commits to it. To discuss an assessment, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

AAL / IAL / FAL

Authenticator, identity and federation assurance levels under the NIST digital identity guidelines (SP 800-63).

FIDO2

A standard for phishing-resistant authentication with security keys or platform passkeys.

ICAM

Identity, credential and access management: the federal term for enterprise identity engineering.

IdP

Identity provider: the system that authenticates users and asserts their identity to applications.

JML

Joiner, mover, leaver: the account lifecycle driven by personnel events.

OIDC / SAML

OpenID Connect and Security Assertion Markup Language: the standard protocols applications use to trust an IdP.

PAM

Privileged access management: vaulting and brokering of administrative credentials.

PIV / CAC

Personal Identity Verification and Common Access Card: the federal and DoD smart-card credentials under FIPS 201.

SCA

Security control assessor: the party that assesses controls, independent of the people who implement them.

SCIM

System for Cross-domain Identity Management: a standard for automated account provisioning.

ZTMM

CISA's Zero Trust Maturity Model, version 2.0.

Appendix B: Illustration Assumptions

All values are planning assumptions for one representative component. None is drawn from a specific agency or a completed engagement.

Assumption	Value	Basis
Portfolio	30 applications, one IdP; 40 alternate	Planning assumption
Legacy share	20% (40% alternate)	Planning assumption
Waves	Pilot of 3, then about 9 per wave	KB range 5–15 per wave
Unit prices	\$8K modern; \$25K legacy	Ends of the \$8K–\$25K band
Engineering effort	32 h per modern app; 100 h per legacy app	Planning assumption
Wave capacity	72 hours a week	Two IAM engineers
App-owner time	8 hours per application	KB range 4–12
Fixed phases	Foundation \$160K, 6 weeks; closeout \$25K, 3 weeks	Inside the \$150K–\$400K foundation band
Assessment	\$55K fixed; 240 hours over 6 weeks	Inside the \$45K–\$95K band
Access lead time	4 weeks, granted during the assessment	Government-furnished

Appendix C: References

1. **Office of Management and Budget**, *M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, January 26, 2022
<https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>

2. **Cybersecurity and Infrastructure Security Agency**, *Zero Trust Maturity Model, Version 2.0*
<https://www.cisa.gov/zero-trust-maturity-model>
3. **Department of Defense Chief Information Officer**, *DoD Zero Trust Strategy*
<https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf>
4. **National Institute of Standards and Technology**, *SP 800-207, Zero Trust Architecture*
<https://csrc.nist.gov/pubs/sp/800/207/final>
5. **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>
6. **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>
7. **General Services Administration**, *Federal Identity, Credential, and Access Management (FICAM) architecture and playbooks*
<https://www.idmanagement.gov/>
8. **FedRAMP**, *FedRAMP Marketplace*
<https://marketplace.fedramp.gov/>
9. **Federal Acquisition Regulation**, *Subpart 9.5, Organizational and Consultant Conflicts of Interest*
<https://www.acquisition.gov/far/subpart-9.5>
10. **DoD Chief Information Officer**, *DoD Cyber Workforce Framework and DoDM 8140.03*
<https://dodcio.defense.gov/Cyber-Workforce/DCWF/>
11. **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/>