

IAM INTEGRATION

Avalon wires your agency's directories, PIV/CAC credentials, and applications into one governed identity system — so every login is phishing-resistant and every access decision is auditable.

THE PROBLEM WE ADDRESS

Fragmented identity is a mission, compliance, and cost risk at once — compromised credentials remain the leading initial-access vector, and orphaned accounts or missing MFA are perennial FISMA and IG findings.

OMB M-22-09 set enterprise identity and phishing-resistant MFA as government-wide requirements, and DoD's Zero Trust Strategy makes identity foundational to 91 activities due by FY2027 — deadlines that outrun agency staffing.

WHAT WE DO

- Identity store inventory and account-hygiene reconciliation
- Identity provider deployment or hardening (Entra ID, Okta for Gov, Ping/ForgeRock)
- Phishing-resistant MFA: PIV/CAC primary, FIDO2/passkey alternative
- Wave-based application integration via SAML 2.0/OIDC and SCIM
- Legacy-application strategies: reverse-proxy, Kerberos delegation, or risk acceptance
- Automated joiner-mover-leaver lifecycle tied to the authoritative HR source
- Access governance: RBAC/ABAC design and access-certification workflows
- Control-implementation evidence mapped to NIST SP 800-53 IA/AC

HOW WE DO IT

1 KICKOFF & DISCOVERY

Stakeholder interviews, identity-store and application inventory, and account-hygiene analysis.

DELIVERABLE

Inventory + hygiene report

3 FOUNDATION & ONBOARDING

Identity provider hardening, PIV/CAC and FIDO2 policy, and wave-based application onboarding.

DELIVERABLE

Applications onboarded

2 TARGET ARCHITECTURE

FICAM-aligned target design, assurance-level selection, and wave sequencing agreed with the ISSM/ZT PMO.

DELIVERABLE

Target architecture + roadmap

4 TRANSITION

Knowledge transfer, admin training, and a closeout brief mapped to POA&M and zero-trust metrics.

HANDOVER

O&M runbook + trained staff

VALUE DELIVERED

- › **A system an auditor can examine.** Every identity store and application feeds one governed platform with logged access decisions.
- › **PIV/CAC past the desktop login.** A per-application integration strategy brings phishing-resistant auth to legacy apps that can't natively federate.
- › **Countable mandate progress.** Wave-based onboarding with per-app runbooks makes FY2027 zero-trust progress reportable, not aspirational.
- › **No platform margin conflict.** Avalon doesn't resell identity licenses, so recommendations serve the agency's own tenancy.

THE ONE THING TO REMEMBER

Founder-level architects do the work directly.

COMMONLY PROCURED AS

Identity & access management (IAM/ICAM) integration services

AT A GLANCE

Model	Fixed-price or T&M, scoped per engagement
Typical	4–7 months for a single-bureau engagement
NAICS	541512, 541511, 541519, 541611, 541690
UEI	Y9MXMMHY3HA1
CAGE	242T0
Standards	NIST SP 800-63-4, OMB M-22-09, CISA ZTMM v2.0, HSPD-12/FIPS 201-3

WHO WE WORK WITH

- › ISSM / Zero Trust PMO lead sequencing identity as a ZT pillar sprint
- › ISSO managing FISMA/IG findings tied to account hygiene or MFA
- › System owner needing legacy applications brought into modern federation

COMMITMENT TO QUALITY

Avalon is led directly by a PMP-certified founder with a decade of enterprise engineering experience where every engagement gets senior-level attention, never a subcontracted bench. Delivery follows NIST SP 800-53, RMF, and FISMA, evidence-backed and control-mapped by design. ISO 9001/27001 is on the roadmap as the pipeline scales.

Status: Small business federal contractor based in Los Angeles, CA

NIST SP 800-63-4

OMB M-22-09

CISA ZTMM V2.0

HSPD-12/FIPS 201-3