



Securing Tomorrow's Missions Today.



Licenses Aren't Maturity: A Fixed-Fee Zero Trust Assessment and Roadmap

Zero Trust Architecture Implementation: find what you already own, score where you stand, and sequence the work that moves the score.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
Why Licenses Are Not Maturity	3
Why It Concentrates in Government	3
The Mandates and the Calendar	5
What the Assessment and Roadmap Does	7
Deliverables	9
What Follows, Conditionally	9
Evidence Assessors Can Use	10
How an Engagement Runs	11
What the Agency Provides	12
What Is Not Included	12
How Avalon Staffs It	13
Pricing and How to Buy	14
Illustration: The Shelfware-to-Maturity Gap	14
The Sequenced Roadmap	16
What the Assessment Costs	16
Common Pitfalls	17
Conclusion and Next Step	17
Appendices	18
Appendix A: Glossary	18
Appendix B: Illustration Assumptions	18
Appendix C: References	19

Executive Summary

Most federal components did not stall on zero trust for lack of tools. They bought identity suites, endpoint agents, secure access licenses and data protection add-ons, often years ago. What they lack is the configuration, the enforcement and the sequence: conditional access policies still in report-only mode, a device compliance policy nobody ties to access, a data loss prevention license that has never seen a policy. The maturity score reflects what is enforced, not what is owned.

The clock has not stopped. OMB M-22-09 set the civilian strategy in January 2022, and CISA's Zero Trust Maturity Model 2.0 remains the yardstick agencies score themselves against. DoD components face target-level zero trust capabilities by the end of FY2027, which as of this writing is the current fiscal year. OMB M-26-14 (May 2026) now sets a risk-based logging model that feeds the visibility pillar, and CISA BOD 26-04 (June 2026) puts risk-based remediation clocks on civilian vulnerabilities.

This paper is for the people who own that gap: component CISOs and zero trust program leads, CIOs who fund the roadmap, ISSMs and ISSOs who keep authorizations valid while the architecture changes, and the CORs who buy the work. It describes Avalon Technology Services' Zero Trust Architecture Implementation service, which starts with one engagement:

- **A fixed-fee Assessment and Roadmap.** A baseline of one bureau or component against CISA ZTMM 2.0 (or the DoD roadmap), a NIST SP 800-207 target architecture, and a dependency-ordered roadmap that separates configuration work from procurement. For a single bureau, typically 7 to 10 weeks of work after kickoff, priced inside a \$45K to \$95K entry band; broader scopes run longer and price higher.
- **Conditional follow-ons.** Architecture design and pillar implementation sprints, scoped from the roadmap, bought only if the agency chooses. Sprints large enough to exceed the simplified acquisition threshold are delivered as a subcontractor to a prime.

Section 9 works through an illustrative bureau that owns 21 of the 24 capabilities its target stage needs. Ten of those 21 are licensed but never deployed, a shelfware ratio of 48%, and 17 of the 20 gaps are configuration work rather than purchases. The fixed fee for that assessment is \$90K.

The service implements and evidences. It does not certify zero trust maturity, grant an authorization or assess its own work; those belong to the agency's assessor, its Authorizing Official and, for DoD, the Department's own validation process.

Why Licenses Are Not Maturity

Zero trust reporting asks what the environment enforces. Procurement records answer a different question: what the agency owns. The gap between the two is where most stalled programs sit, and it shows up in the same ways across components.

Symptom	What it usually means
"We bought the licenses; nobody turned the policies on."	Capabilities owned but never configured. The fix is engineering time and decisions, not money.
Conditional access in report-only mode for a year	Configured but not enforced. Someone has to own the exceptions enforcement will create.
"We can't say how many devices we have."	No reconciled inventory, so device-conditioned access and segmentation have nothing to stand on.
"Once you're in, you're in."	A flat network behind a VPN. The networks pillar sits at Traditional regardless of the identity score.
"Identity and devices are fine; data is a mess."	The common civilian pattern: the data pillar lags while licenses for it sit unused.
"We have 91 activities and three people."	A DoD component with a capacity gap, not a knowledge gap.

Why It Concentrates in Government

- **Licenses arrive in enterprise agreements.** Identity, endpoint and data protection features come bundled. Owning them takes a signature; enforcing them takes design, testing, change approvals and someone to adjudicate exceptions.
- **Every change rides the change board.** Conditional access and segmentation changes go through the agency's change process. A monthly change board turns a ten-week sprint into sixteen.
- **The ISSM carries the risk.** Each architecture change can touch an authorization boundary. Without a security-impact analysis, the safest answer is to leave policies in report-only mode.

- **Self-scores drift.** A maturity score built from tool lists, not from what is enforced, overstates progress until an inspector general or a real incident tests it.

The Mandates and the Calendar

Driver	What it requires	What it means for the roadmap
OMB M-22-09 (Jan 26, 2022)	Federal civilian zero trust strategy: identity, devices, networks, applications and data goals	The strategy agencies still report progress against; its FY2024 goals have passed, the reporting has not
CISA ZTMM 2.0	Five pillars (identity, devices, networks, applications and workloads, data) plus visibility and analytics, automation and orchestration, and governance; stages Traditional, Initial, Advanced, Optimal	The civilian measuring stick for the baseline and the re-score
NIST SP 800-207	Zero trust architecture: policy decision and enforcement points, tenets for access decisions	The design basis for the target architecture; guidance, not a standard anyone passes
DoD Zero Trust Strategy	Target-level zero trust capabilities across seven pillars by the end of FY2027	September 30, 2027 is the planning horizon for every DoD component roadmap
OMB M-26-14 (May 2026)	Risk-based logging model; replaced M-21-31	Logging comes before analytics; the visibility pillar's sprint follows it
CISA BOD 26-04 (Jun 10, 2026)	Risk-based remediation clocks for civilian agencies, from 3 days with forensic triage to the next upgrade	Device and inventory work feeds the same asset data the remediation clocks depend on
TIC 3.0	Trusted internet connection use cases for modern architectures	VPN and TIC refresh moments are natural points to move to identity-aware access

Driver	What it requires	What it means for the roadmap
DoD CSRMC (Sep 24, 2025)	Cybersecurity risk management construct announced; RMF, DoDI 8510.01 and eMASS remain in use	Evidence still goes into the RMF record the component uses today

Two buying moments recur. Fiscal year-end (July through September) favors assessment-sized purchases with expiring operations funds. The FY2028 budget build needs a roadmap that reads as budget justification. A credential compromise, an inspector general finding or a VPN end-of-life can move either date forward.

What the Assessment and Roadmap Does

The entry engagement answers three questions for one bureau or component: where each pillar actually stands, what the target architecture should look like, and what order of work moves the score with the tools the agency already owns.

Workstream	Activities
Maturity baseline	Score each pillar against CISA ZTMM 2.0, or the DoD roadmap for DoD components, through document and SSP review, architecture walkthroughs, interviews and tool-deployment verification
Owned versus enforced	For every capability the target stage needs, record whether it is licensed only, configured (report-only, pilot or partial), enforced, or not owned, from license exports and configuration evidence
Target architecture	An agency-specific NIST SP 800-207 architecture: where policy decision and enforcement points sit, how identity and device signals feed access decisions, macro-segmentation of enclaves first and micro-segmentation of high-value assets second, an identity-aware proxy pattern for legacy applications, and the data protection approach
Roadmap and investment plan	Budget-cycle-sized phases, dependency-ordered (identity before device-conditioned access; inventory before segmentation; logging before analytics), with configuration-only activities separated from procurement

Deliverables

Deliverable	Format
Maturity assessment report with pillar-by-pillar scoring and gap analysis	PDF report and executive briefing
Owned-versus-enforced capability register	Spreadsheet, one row per capability, with the evidence behind each status
Target-state reference architecture	Diagrams (Visio or draw.io source and PDF) with a design narrative
Roadmap and investment plan	Phased spreadsheet and briefing usable as budget justification
Control and activity traceability	Draft mapping of planned changes to 800-53 controls and ZTMM or DoD activities

The roadmap is written to be specification-neutral. It names capabilities and outcomes, not products, so the agency can compete any follow-on work, including against Avalon.

What Follows, Conditionally

If the agency chooses to continue, the roadmap scopes two kinds of follow-on work. Detailed design turns the reference architecture into build-ready specifications. Pillar sprints implement it in the agency's own tooling: identity first in nearly every case (phishing-resistant MFA, conditional access, privileged access), then devices (inventory reconciliation, compliance-conditioned access), then network segmentation, with application and data work interleaved. Each sprint ends with deployed configurations, exported policy definitions, as-built runbooks, a control-mapped evidence package, knowledge transfer and a re-score against the same model used at baseline. None of this is committed by buying the assessment.

Evidence Assessors Can Use

Control	Evidence the follow-on work produces
AC-2, AC-3, AC-6	Conditional access and least-privilege policy definitions; account and role reviews
AC-4, SC-7	Segmentation design and rule sets; host-to-host reachability test results
AC-17	Identity-aware remote access configuration replacing broad VPN access
IA-2, IA-5, IA-8	Phishing-resistant MFA enforcement records; authenticator and federation configuration
SC-8, SC-23	Internal traffic encryption and session protection settings
AU-2, AU-6, AU-12	Pillar telemetry routed to the SIEM, aligned to the agency's M-26-14 logging approach
CM-8	Reconciled asset inventory used by device-conditioned access
SI-4	Monitoring coverage for enforcement points

For systems that process CUI, the same work maps to NIST SP 800-171 families 3.1, 3.5 and 3.13. Allowed and denied access matrices and segmentation reachability tests show that policies behave as designed. They are implementer artifacts. The agency's assessor draws the assessment conclusions, and the Authorizing Official makes the authorization decision. Significant architecture change can trigger reassessment, so Avalon coordinates a security-impact analysis with the ISSM before each enforcement change.

Accurate	Not accurate
Implements controls mapped to named 800-53 controls and ZTMM or DoD activities	Achieves compliance with M-22-09
Advances the identity pillar from Initial toward Advanced	Zero trust certification
Positions the component to complete named target-level activities	Guarantees target level by FY2027
Produces evidence for the assessor	Results in an ATO

How an Engagement Runs

Phase	Typical duration	What happens
Kickoff and access	1–3 weeks	Sponsor alignment, account requests, data call for SSPs, diagrams, inventories and license exports
Baseline	3–6 weeks	Interviews, configuration review, owned-versus-enforced register, pillar scoring
Architecture and roadmap	4–8 weeks	Reference architecture, segmentation model, legacy-application pattern, phased plan
Pillar sprint (optional follow-on)	8–16 weeks each	Implementation in the agency's tooling, monitor mode first, then enforcement
Validation and closeout (with sprints)	3–5 weeks	Allowed and denied testing, segmentation checks, re-score, evidence package, knowledge transfer

Assessment through two implemented pillars at component scale typically runs six to nine months. Department-scale, all-pillar programs run two to four years and are large-integrator work; Avalon's role there would be a defined workstream under a prime.

What the Agency Provides

- A sponsor with decision authority, usually the CISO or deputy, who can decide access-policy questions within days. Zero trust changes who can reach what, and someone has to own the exceptions.
- Accounts and any required credential sponsorship within a stated window. The schedule starts when access is granted, not at award.
- Identity, network and endpoint administrators for four to eight hours a week each during their pillar's work, and system owners for the applications in scope.
- Current SSPs, network diagrams, asset inventory exports, prior assessment results and license inventories.
- Change board throughput for any follow-on enforcement work, stated in the schedule.

What Is Not Included

Included	Separate work
Vendor-agnostic assessment, design and configuration in the agency's tools	Product or license procurement and resale
Routing pillar telemetry to the agency SIEM	Security operations center monitoring and alert triage
Evidence for the assessor and the authorization record	Control assessment, authorization, certification or DoD target-level validation
Access-policy and segmentation functional testing	Penetration testing of the implemented controls, which needs an independent party
Identity as one pillar among several	A standalone identity modernization program
Integration with data the agency's CDM program provides	Operating a CDM capability
Unclassified environments	Classified enclaves and cross-domain work

How Avalon Staffs It

Avalon takes one engagement at a time and works in unclassified environments only. The Assessment and Roadmap is led by a zero trust architect at 0.75 to 1.0 FTE, with a compliance specialist and a project manager at a quarter-time each. Avalon has no past federal engagements under this service, and it cites no credential, clearance or past engagement that is not current and verifiable.

Requirement	How it is handled
Architecture lead	Named personnel whose certifications and investigation level match the agency's requirements, listed in the proposal
Platform depth for sprints	Engineers with configuration depth on the agency's actual identity, endpoint and network stack, named in the proposal, hired or subcontracted, as a condition of any sprint
DoD privileged access	Personnel qualified under DoD 8140 for the relevant work role, as a condition of the engagement
Civilian access	Public Trust investigation at the tier the agency requires, as a condition of the engagement
Segmentation at scale	Not offered by Avalon as sole performer; delivered as part of a prime's team where needed
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	Pricing basis
Assessment and Roadmap, one bureau or component	\$45K–\$150K	Firm fixed price
Avalon entry offer, one bureau	\$45K–\$95K	Firm fixed price
Detailed design (conditional follow-on)	\$100K–\$350K	Firm fixed price
Single-pillar implementation sprint (conditional)	\$250K–\$900K	Time and materials with a ceiling, or fixed price

The Assessment and Roadmap and most design work fit under the \$350,000 simplified acquisition threshold, so they can be bought as open-market purchases with one-year funds. 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. A sprint above the threshold, or zero trust 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.

Performance-based pricing tied to a maturity score is declined, because the score depends on agency decisions and change approvals the contractor does not control. Fixed fee against a defined scope keeps the incentives clean.

Illustration: The Shelfware-to-Maturity Gap

The figures below are a planning illustration for one representative bureau, not a quote and not a result from any engagement. Every capability count and status is an assumption.

The bureau needs a defined set of capabilities to reach its target stage in each pillar. The baseline tags each one: **enforced**, **configured** (deployed but report-only, pilot or partial), **licensed only** (owned, never deployed) or **not owned**. The shelfware ratio is licensed-only capabilities divided by owned capabilities.

Pillar	Stage now to target	Owned	Enforced	Unused	Shelfware	Config	Buy
Identity	Initial to Advanced	5	1	2	40%	4	0
Devices	Initial to Advanced	3	1	1	33%	2	1
Networks	Traditional to Initial	3	0	1	33%	3	1
Applications and Workloads	Traditional to Initial	2	0	1	50%	2	1
Data	Traditional to Initial	4	1	3	75%	3	0
Visibility, Analytics, Automation	Initial to Advanced	4	1	2	50%	3	0
Total		21	4	10	48%	17	3

Unused: licensed but never deployed. Shelfware: unused divided by owned. Config: gaps closed by configuration alone. Buy: capabilities that must be procured.

Read across the totals. The bureau owns 21 of the 24 capabilities it needs and enforces only 4. Ten are shelfware (48%), and another 7 are deployed but not enforced, so 81% of what it owns does not yet count toward maturity. Of the 20 gaps between now and target, 17 (85%) are configuration-only and 3 require a purchase.

The data pillar shows the pattern most sharply: three of its four capabilities are licensed and unused, a 75% shelfware ratio, and nothing needs to be bought. Networks is the opposite: every owned capability is short of enforcement, and micro-segmentation of high-value assets is a real purchase that waits for a reconciled inventory.

The Sequenced Roadmap

Order	Pillar	Config-only	Buy	Why here
1	Identity	4	0	Every access decision depends on identity
2	Devices	2	1	Inventory and posture before device-conditioned access
3	Networks	3	1	Segmentation needs the inventory first
4	Applications and Workloads	2	1	Onboard apps to the identity controls already enforced
5	Data	3	0	Policies first; licenses already owned
6	Visibility, Analytics, Automation	3	0	Logging before analytics and automation

The configuration-only rows are the budget argument. They need engineering time, decisions and change approvals, not new money for tools. The procurement rows are few, specific and sequenced behind the work that makes them usable.

What the Assessment Costs

Scenario	Weeks of work	Award to done	Rate-band range	Fixed fee
Narrow (three pillars, 0.75 FTE architect)	7	8–10 weeks	\$53K–\$76K	\$64K
Base (all pillars, one bureau)	8	9–11 weeks	\$74K–\$106K	\$90K
Broad (adds DoD roadmap crosswalk, more enclaves)	12	13–15 weeks	\$112K–\$160K	\$134K

In the base case, 8 weeks of work (four of baseline, four of architecture and roadmap) at mid-band rates price at \$90K, inside the \$45K to \$95K entry band and well under the simplified acquisition threshold. A narrower scope comes in lower. A broad scope that adds a DoD roadmap crosswalk and more enclaves prices near \$134K: still inside the market range and under the threshold, but above Avalon's entry band, so it is better split by enclave or priced as its own fixed-fee scope than squeezed into the entry offer.

Common Pitfalls

Pitfall	How to avoid it
"Implement zero trust" as the scope	Name the bureau, the pillars, the maturity model and the deliverables; anything else is unpriceable
The legacy-application rabbit hole	Cap the number of applications in scope and price additional ones per application
Tool procurement drift	Run the owned-versus-enforced register before any purchase; buy only what the roadmap calls for
Operations absorbing the change	Time-box post-enforcement support to about two weeks and hand over runbooks the SOC can use
Enforcement that breaks an authorization	Monitor mode first; security-impact analysis with the ISSM before each enforcement change
Conflict of interest on follow-ons	A specification-neutral roadmap, disclosed in writing, so follow-on work can be competed

Conclusion and Next Step

Zero trust maturity moves when policies are enforced, not when licenses are bought. For most components the fastest gains are already paid for: capabilities sitting in report-only mode or never deployed, waiting for design decisions, a sequence and someone to own the exceptions. A baseline that separates what is owned from what is enforced turns a vague mandate into a short list of configuration work and an even shorter list of purchases.

The natural first step is the fixed-fee Assessment and Roadmap: one bureau, a defined scope under the simplified acquisition threshold, an owned-versus-enforced register, a NIST SP 800-207 target architecture, and a roadmap the agency can compete and

fund. To discuss an assessment, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

Conditional access

Policies that grant or deny access based on identity, device and session signals.

Monitor (report-only) mode

A policy that records what it would have blocked without blocking it; used before enforcement.

PDP and PEP

Policy decision point and policy enforcement point: where an access decision is made and where it is applied (NIST SP 800-207).

Shelfware ratio

In this paper, licensed-only capabilities divided by all owned capabilities in a pillar.

ZTMM

CISA's Zero Trust Maturity Model, version 2.0: five pillars, three cross-cutting capabilities and four stages.

ZTNA

Zero trust network access: identity-aware access to applications, typically replacing broad VPN access.

Micro-segmentation

Restricting traffic between individual workloads or hosts, applied first to high-value assets.

Appendix B: Illustration Assumptions

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

Assumption	Value	Basis
Capabilities needed for target	24 across five pillars and the cross-cutting capabilities	Planning assumption
Status mix	4 enforced, 7 configured, 10 licensed only, 3 not owned	Planning assumption
Stages	Identity, devices and cross-cutting Initial to Advanced; networks, applications and data Traditional to Initial	Planning assumption
Team loading	Architect 0.75–1.0 FTE; compliance 0.25; PM 0.25; 40 hours a week	KB delivery model
Rates	Architect \$175–\$250; compliance \$120–\$170; PM \$110–\$160 an hour; fee at mid-band	KB market-norm bands
Durations	Kickoff 1–3 weeks; baseline 3–6; architecture and roadmap 4–8	KB phase durations
Price check	Base fee \$90K	Inside the \$45K–\$95K entry band

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. **National Institute of Standards and Technology**, *SP 800-207, Zero Trust Architecture*
<https://csrc.nist.gov/pubs/sp/800/207/final>

4. **Department of Defense Chief Information Officer**, *DoD Zero Trust Strategy*
<https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf>
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 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
<https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final>
7. **Cybersecurity and Infrastructure Security Agency**, *Trusted Internet Connections (TIC) 3.0*
<https://www.cisa.gov/resources-tools/programs/trusted-internet-connections-tic>
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. **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/>