



Securing Tomorrow's Missions Today.



The Interface Nobody Documented: A Fixed-Fee Interface Census and API Target Design for One Mission System

Web Services & Microservices: every interface named and dispositioned, the first APIs specified contract-first, and a priced build plan the ISSO has already reviewed

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
Why Interfaces Become the Bottleneck	3
Why Integration Projects Stall	3
The Mandates and the Calendar	5
What the Engagement Does	6
The Interface Disposition	6
Contract-First API Design	7
Deliverables	7
Where the Engagement Stops	7
Evidence the ISSM Can Use	8
How an Engagement Runs	9
What the Agency Provides	10
What Is Not Included	10
How Avalon Staffs It	10
Pricing and How to Buy	12
Illustration: One System, Five Weeks	12
Labor Loading	13
What the Engagement Costs	13
What the Agency Brings to the Readout	14
Common Pitfalls	14
Conclusion and Next Step	15
Appendices	15
Appendix A: Glossary	15
Appendix B: Illustration Assumptions	15
Appendix C: References	16

Executive Summary

Most federal mission systems have more interfaces than anyone can list. A nightly batch file feeds the payment system. A fifteen-year-old SOAP service answers a reporting tool. Another program reads the database with a shared login. Staff re-key records into a second system because no connection exists at all. Each link was built contract by contract, and few were documented. When the agency needs that system's data somewhere new, the first question is one nobody can answer: what is connected to it today?

The pressure to answer is growing. Zero trust plans under OMB M-22-09 and the CISA Zero Trust Maturity Model 2.0 call for per-request authorization and encrypted traffic at the application and workload layer, which shared logins and file drops cannot provide. OMB M-26-14 (May 2026) asks for risk-based logging decisions, and an undocumented interface logs nothing useful. SQL Server 2016 support ended July 14, 2026 and Windows Server 2016 support ends January 12, 2027, so many legacy interfaces need rework anyway.

This paper is for the system owner who funds the system, the CIO or chief architect who sets the integration pattern, the ISSM or ISSO who carries the boundary, the chief data officer when data sharing drives the need, and the COR who buys the work. It describes Avalon Technology Services' Web Services & Microservices service, which starts with one engagement:

- **A fixed-fee interface census and API target design for one named system.** One unclassified system, about five weeks. Every point-to-point link, file drop, batch job, SOAP service and shared database login is named and given a disposition: keep, facade, API, event or retire. The top three interfaces get OpenAPI 3.x specifications, the gateway and security design is reviewed with the ISSO before any code is written, and the engagement ends with a priced firm-fixed-price build plan. The market band is \$25K to \$75K; Avalon's anchor is \$30K to \$60K.
- **A conditional build follow-on.** The APIs and facades the plan specifies, built on the agency's existing gateway and platform. A small build (one source system, a handful of endpoints) typically runs \$75K to \$250K firm fixed price.

The illustration later in this paper works through the effort model. The base case is 12 interfaces and 3 priority APIs over five weeks: 322 hours at market-norm rates, or \$48.2K to \$68.7K, with a \$58K planning fee, well under the \$350,000 simplified acquisition threshold.

Avalon designs and documents. The authorization decision remains the government's; Avalon does not issue or guarantee an ATO, assess its own work, or certify compliance.

Why Interfaces Become the Bottleneck

Any two of these phrases in one meeting usually mean the interface layer, not the application, is the problem.

What the program says	What it usually means
"We re-key the same data into three systems."	No interface exists, so staff time is the integration
"The nightly job failed again and the field couldn't work until noon."	A batch file carries mission data with no retry, alerting or owner
"Only one person understands that interface, and he's a contractor."	The interface documentation is one person's memory
"Every change request on that system takes nine months."	Consumers are wired to internals, so every change breaks someone
"The mobile app project is stuck waiting on the back end."	The system has no API for a new front end to call

One routing question separates this service from its parent. If the pain is that the agency **can't get data out** of the system, the answer is an interface layer, and this engagement fits. If the pain is that the agency **can't change the system safely**, the answer is usually decomposition or replacement, which is Avalon's separate Application Modernization service.

Why Integration Projects Stall

- **Nobody counts the interfaces first.** The file drop nobody mentioned surfaces in testing.
- **Code comes before the contract.** Consumers negotiate with the implementation instead of a specification.
- **Security review arrives late.** The ISSO sees the design at the end, and the work waits for an impact analysis nobody scheduled.

- **Data cleanup hides inside integration.** When the source data is poor, the project quietly becomes a data-quality effort with no end.
- **Decomposition becomes the goal.** Many small services add operating cost the agency may not carry. A well-facaded system is often the right end state.

Engineers who lived through service-oriented architecture raise a fair objection. Those programs mostly failed on governance and topology: a heavy central bus, committee-built data models and locked-in middleware. Contract-first specifications and decentralized data ownership invert those choices. Microservices are not the goal; decoupling is.

The Mandates and the Calendar

Driver	What it says	What it means for this engagement
OMB M-22-09, CISA Zero Trust Maturity Model 2.0, DoD Zero Trust Strategy	Civilian strategy with an applications and workloads pillar; DoD target-level capabilities by the end of FY2027	Gateway-fronted APIs carry per-request authorization to the interface layer
NIST SP 800-204 series	Security strategies for microservices and service mesh	The methodology the design cites
OWASP API Security Top 10	The common API weaknesses	The checklist each design is reviewed against
OMB M-26-14 (May 2026)	A risk-based logging model; replaced M-21-31	The gateway design states what each API logs and where it goes
CISA BOD 26-04 (Jun 10, 2026)	Risk-based remediation clocks; replaced BOD 22-01 and BOD 19-02	Interfaces on unpatchable components cannot meet the clocks
Windows Server 2016 and SQL Server 2016	SQL Server 2016 support ended July 14, 2026; Windows Server 2016 support ends January 12, 2027	The cheapest time to redesign their interfaces
Evidence Act and 21st Century IDEA Act (2018)	Machine-readable data access and modern digital services	Both presuppose APIs; this work enables them, it does not satisfy them
FedRAMP Consolidated Rules (Jun 25, 2026)	Cloud offerings are "FedRAMP Certified" in classes A through D; certification covers the provider's offering only	A certified gateway or platform passes down controls; custom APIs fall under the agency's own authorization

One note on software assurance. OMB M-26-05 (January 23, 2026) rescinded M-22-18 and M-23-16. Agencies now set their own risk-based software assurance policies, NIST SP 800-218 (the Secure Software Development Framework) is guidance, the CISA attestation form is optional, and an SBOM is a contract term the agency may choose for the APIs it buys. Avalon can deliver SBOMs for built components when the agency asks.

What the Engagement Does

The engagement covers one named system and works in the agency's own repositories, gateway and tools.

Step	Activities
Interface census	Every point-to-point link, file drop, batch job, SOAP service, shared database login and manual re-keying step, named and counted, with owner, protocol, schedule and data sensitivity
Data-access confirmation	Which tables, transactions or services each interface touches, plus a data-profiling sample with issues recorded, not fixed
Disposition	Keep, facade, API, event or retire for every interface, with the reasoning written down
Contract-first API design	OpenAPI 3.x specifications for the top three interfaces, an API style guide and a versioning and deprecation policy
Gateway, security design and build plan	Gateway policy reviewed with the ISSO as a milestone; endpoints, acceptance criteria and a firm-fixed-price estimate for the follow-on

The Interface Disposition

Each interface ends with one of five decisions. **Keep**: it works, is documented and carries acceptable risk. **Facade**: a REST layer goes in front of something that cannot change, such as a SOAP service or legacy database, so consumers modernize before the source does. **API**: a gateway-fronted service replaces the point-to-point link. **Event**: a message broker replaces a nightly batch file. **Retire**: nobody uses it, and the census proves it. A large share of federal interfaces are still SOAP; the census treats them as assets to wrap, not to rip out.

Contract-First API Design

For the three interfaces that matter most, the specification comes before any code. Each OpenAPI 3.x file defines resources, schemas, error codes and examples, and lives in the agency's repository so consumers and builders share one contract. Authentication is OAuth 2.0 or OpenID Connect tied to the agency's identity, credential and access management (ICAM) service, including PIV- or CAC-derived credentials where the agency uses them. The gateway enforces token validation, rate limits, schema validation and logging as configuration in code, never set by hand in a console.

Deliverables

Deliverable	Format
Interface register with disposition per interface	XLSX register and a summary report
OpenAPI 3.x specifications for the priority interfaces	YAML files in the agency repository
API style guide and versioning and deprecation policy	Governance document
Gateway and security design, data flow diagrams, ports, protocols and services matrix	Design document, editable diagrams
Draft interface control documents (ICDs) for the priority interfaces	The agency's ICD format
Data-profiling report	PDF
Priced build plan	Document and estimate

Where the Engagement Stops

The engagement stops at the build plan. Whether to rewrite or retire the system is Application Modernization; portfolio disposition is IT Modernization; moving workloads is Cloud Migration. New services are Cloud Native Development, the landing zone or Kubernetes platform is Cloud Architecture & Engineering, the pipeline belongs to CI/CD Pipelines and DevSecOps, and zero trust program design is its own service. Each is a separate Avalon service, as are the SSP and ATO workstreams. Source-data cleanup, user interface work and license resale are out of scope.

Evidence the ISSM Can Use

Control	What the design and follow-on address
AC-3, AC-4	Access enforcement and information flow enforcement through gateway policy
SC-7, SC-8	Boundary protection at the gateway; TLS on every interface and mutual TLS between services where a mesh exists
IA-2, IA-8	Authentication of organizational and non-organizational users through OAuth 2.0 or OIDC tied to agency ICAM
AU-2, AU-12	Defined audit events and log generation at the gateway, set to the agency's M-26-14 decisions
SI-10	Input validation through schema enforcement at every API boundary
CM-2, CM-3	Gateway configuration as code, so the baseline and every change are versioned

The accurate statement is narrow: this effort designs and documents interface- and workload-layer controls (AC-3, AC-4, SC-7, SC-8, IA-2, AU-12, SI-10) and delivers architecture and evidence artifacts for the system's security authorization. It does not itself constitute an assessment, an authorization or a certification. The census also shows the ISSO the shared logins and file drops already crossing the boundary unmanaged.

Accurate	Not accurate
Names every interface that crosses the boundary	Achieves zero trust
Produces data flows and a ports, protocols and services matrix for the SSP	Delivers an ATO
Designs gateway policy the ISSO reviewed before build	Makes custom APIs "FedRAMP authorized"
An input to the ISSM, the assessor and the AO	Guarantees an assessment outcome

Agencies do not authorize many small services one at a time. One boundary can hold many services, platform controls on the cluster, mesh and pipeline are inherited by each, and each new service adds a thin layer of system-specific evidence. The target design keeps the boundary and inheritance model in view from week one.

How an Engagement Runs

Phase	Timing	What happens
0: Kickoff and access	Award, in parallel	Repository, documentation and lower-environment access; SMEs named; dependencies dated in writing
1: Interface census	Weeks 1–3	Inventory, data-access confirmation, profiling samples and SME interviews
2: Disposition and API design	Weeks 3–5	Dispositions, OpenAPI specifications, gateway and security design, ISSO review, priced build plan and readout
3–5: Build, hardening and transition (separate, conditional)	About 9–20 weeks	Build and integrate, security and load testing, acceptance, runbooks and knowledge transfer

A full interface engagement typically runs 10 to 24 weeks, scaling with integration points and how opaque the legacy sources are, not with agency headcount. The census is

Phases 1 and 2 only, bought as a standalone firm-fixed-price task. Firm-fixed-price the design, then price the build firm fixed once the design has bounded the unknowns.

What the Agency Provides

- Access to the source system, its documentation and interface owners, dated at award.
- Named legacy SMEs with real calendar time. SME availability is the most common schedule risk in this work, so their hours go into the statement of work.
- A lower environment, or the authority to request one, for data-access checks.
- The ISSO or ISSM at the design review, scheduled as a milestone.
- A sponsor who can move firewall and network changes through the change board, submitted in week one.

What Is Not Included

Included	Separate work
Census, dispositions and API design for one system	Interfaces across a portfolio of systems
Priced build plan	The build, unless bought as the follow-on
Data-profiling report	Fixing the source data
Unclassified systems	Classified, IL5 or cleared environments

How Avalon Staffs It

Avalon takes one engagement at a time, works business hours, and works on unclassified systems only. Avalon's founder leads the engagement. The solutions architect and software engineer are named personnel, hired or subcontracted for the engagement and listed in the proposal with their résumés; without a named architect, Avalon bids facade scope only. 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 named team, a fixed price, verifiable acceptance criteria and a small first increment.

Requirement	How it is handled
Solutions architect	Named personnel whose certifications and investigation level match the agency's requirements, listed in the proposal
Software engineer	Named in the proposal; a build follow-on needs two or more engineers confirmed before it is bid
Privileged access on DoD systems	The DoD 8140 qualification the program requires, as a condition of the engagement
Civilian access	Public Trust investigation at the tier the agency requires
Platform and tooling	The agency's repositories, gateway and documentation tools, with access the agency provisions; Avalon hosts nothing
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

Key personnel substitution requires CO approval. Delivered specifications, configurations and documents belong to the agency from the first day, with data rights under FAR 52.227-14 or DFARS 252.227-7014 as the contract specifies.

Pricing and How to Buy

Engagement	Market-norm range	Avalon
Interface census and API target design, one system, about 5 weeks	\$25K–\$75K	Firm fixed price within \$30K–\$60K for the base scope; illustrative \$58K
Small build: one source system, a handful of endpoints, existing gateway	\$75K–\$250K	Conditional follow-on, firm fixed price against the build plan
Medium build: gateway stand-up or several integrations across 2–3 systems	\$250K–\$750K	Only with a confirmed engineering bench
Meaningful monolith decomposition	\$750K and up	Scoped as Application Modernization, not this service

The census sits under the \$350,000 simplified acquisition threshold and can be bought as an open-market purchase. Larger build work can be subcontracted to Avalon by a prime. Avalon does not hold a GSA Schedule or a governmentwide contract today, and it does not resell hardware, software, gateway licenses or support.

Integration work is usually funded from single-year operations and maintenance money, which makes a short census a natural third- or fourth-quarter purchase. Prices are fixed against one named system, a capped interface count and a capped number of API specifications, with a dated dependency schedule.

Illustration: One System, Five Weeks

The figures below are a planning illustration for one representative unclassified system: a case management system that feeds a payment system, a reporting warehouse and a partner agency, connected through nightly batch files, two SOAP services, a shared database login and manual re-keying. They are not a quote and not a result from any engagement.

Labor Loading

Each interface takes about 4 architect and 4 engineer hours to trace, check and disposition. Each priority API takes about 8 architect and 32 engineer hours to specify. A fixed 40 architect hours cover the ISSO review, gateway policy, style guide and build plan, plus 16 DevSecOps hours on the existing gateway configuration; the project manager is at one-quarter time.

Role	Rate band	Base hours
Solutions architect	\$175–\$250/hr	112
Senior software engineer	\$140–\$200/hr	144
DevSecOps engineer	\$150–\$210/hr	16
Project manager	\$120–\$170/hr	50
Total		322

What the Engagement Costs

Scope	Hours	Rate-band range	Planning fee	Inside \$25K–\$75K
Small (8 interfaces, 2 APIs, 4 weeks)	240	\$36.0K–\$51.4K	\$44K	Yes
Base (12 interfaces, 3 APIs, 5 weeks)	322	\$48.2K–\$68.7K	\$58K	Yes
Large (20 interfaces, 4 APIs, 7 weeks)	446	\$66.5K–\$94.9K	\$81K	No: cap or split

The base case is 322 hours, or \$48.2K to \$68.7K, with a \$58K planning fee at the midpoint. The fee sits inside the \$25K to \$75K market band and Avalon's \$30K to \$60K anchor; the top of the rate band does not, which is why the statement of work caps the interface count at 12 and the API specifications at 3. The small case runs \$36.0K to

\$51.4K. The 20-interface case runs \$66.5K to \$94.9K and breaks the market band, so a system that large is split or priced per added interface.

At these rates, each interface beyond the cap adds about \$1.3K to \$1.8K for inventory and disposition, and each added API specification adds about \$5.9K to \$8.4K. Where even the count is unknown, a short time-and-materials discovery ahead of the fixed price is the honest alternative to padding.

What the Agency Brings to the Readout

The model prices the census; it claims no saving. The size of the problem comes from the agency's own numbers: records re-keyed each month, times the minutes each one takes, times twelve. At an illustrative 2,000 records a month and six minutes each, that is 2,400 staff hours a year, about 1.4 full-time staff. Add the hours of field work lost each time a batch job fails. Those figures, not a vendor estimate, go to the budget office.

Common Pitfalls

Pitfall	How to avoid it
"While you're connected, add one more integration"	Named interfaces and a countable endpoint list; additions by priced modification
Data cleanup posing as integration	The API exposes source data as it is; the profiling report records issues without an obligation to fix them
Undocumented interfaces found mid-build	A paid census before the fixed-price build, and a change mechanism for count changes
"Can you just build a small screen for it?"	User interface work named as out of scope
Warranty support that never ends	A defined warranty period and defect definition; operations beyond it are a follow-on
Compliance oversell	No claim that a gateway achieves zero trust or that the work delivers an ATO

Conclusion and Next Step

Most systems that cannot share their data are not missing technology. They are missing a list: which interfaces exist, which matter, and what each should become.

The natural first step is the fixed-fee interface census: one named system, about five weeks, under the simplified acquisition threshold, ending in an interface register with a disposition for every link, contract-first specifications for the first APIs, a gateway design the ISSO has reviewed and a priced build plan. To discuss a system, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

API gateway

The policy enforcement point in front of an agency's APIs.

Contract-first design

Writing the API specification before the code, so consumers and builders share one contract.

Facade

A modern API placed in front of a system or service that cannot be changed directly.

ICD

Interface control document: the agency-format record of how two systems exchange data.

Strangler-fig pattern

Moving functions from a legacy system to new services one slice at a time while the legacy system keeps running.

Appendix B: Illustration Assumptions

All values are planning assumptions for one representative unclassified system. None is drawn from a specific agency, a real system or a completed engagement.

Assumption	Value	Basis
System	One mission system with mixed batch, SOAP, shared-database and manual interfaces	Planning assumption
Scope caps	12 interfaces, 3 API specifications	Planning assumption
Per-interface effort	4 architect and 4 engineer hours	Planning assumption
Per-API effort	8 architect and 32 engineer hours	Planning assumption
Fixed effort	40 architect, 16 DevSecOps hours; PM 0.25 FTE	KB delivery model; hours assumed
Rates	Architect \$175–\$250, engineer \$140–\$200, DevSecOps \$150–\$210, PM \$120–\$170 an hour	Market-norm rate bands
Price check	Base fee \$58K	Inside \$25K–\$75K and \$30K–\$60K; under the SAT

Appendix C: References

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 800-204, Security Strategies for Microservices-based Application Systems*
<https://csrc.nist.gov/pubs/sp/800/204/final>
7. **National Institute of Standards and Technology**, *SP 800-204A, Building Secure Microservices-based Applications Using Service-Mesh Architecture*
<https://csrc.nist.gov/pubs/sp/800/204/a/final>
8. **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>

9. **OWASP Foundation**, *OWASP API Security Top 10*
<https://owasp.org/API-Security/>
10. **Cybersecurity and Infrastructure Security Agency**, *Zero Trust Maturity Model, Version 2.0*
<https://www.cisa.gov/zero-trust-maturity-model>
11. **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>
12. **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>
13. **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>
14. **Microsoft**, *Windows Server 2016 and SQL Server 2016 lifecycle*
<https://learn.microsoft.com/en-us/lifecycle/products/>
15. **FedRAMP**, *FedRAMP program and 2026 Consolidated Rules*
<https://www.fedramp.gov>
16. **U.S. Congress**, *21st Century Integrated Digital Experience Act (H.R. 5759, 115th Congress)*
<https://www.congress.gov/bill/115th-congress/house-bill/5759>
17. **U.S. Congress**, *Foundations for Evidence-Based Policymaking Act of 2018 (H.R. 4174, 115th Congress)*
<https://www.congress.gov/bill/115th-congress/house-bill/4174>
18. **Acquisition.gov**, *FAR 15.305, Proposal evaluation*
<https://www.acquisition.gov/far/15.305>
19. **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/>