AVALON
TECHNOLOGY SERVICES

Securing Tomorrow's Missions Today.

2026

You Already Run Open Source. Can You Say Which Parts? A Fixed-Fee Open-Source Inventory and Governance Assessment for One Program

Open-Source Technologies: learn which components your systems run, who supports them, which licenses need counsel, and which proprietary renewals deserve a migration case

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary **2**

Why Programs Cannot Say What They Run **3**
Four Misconceptions 3

The Policies and the Calendar **5**

What the Assessment Does **7**
Three Support Tiers 7
Migration Candidates 8
Deliverables 9
Where the Engagement Stops 9

Evidence the ISSM and the CIO Can Use **10**

How an Engagement Runs **11**
What the Agency Provides 11
What Is Not Included 12

How Avalon Staffs It **12**

Pricing and How to Buy **13**

Illustration: One Program, Three Systems **14**
Components 14
Platform Support Tiers 15
Proprietary Renewals 15
What the Engagement 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

Every federal program already runs open source software. Linux, PostgreSQL, OpenJDK, Kubernetes and thousands of smaller libraries sit inside systems that were authorized years ago, many of them pulled in by a developer or a vendor without anyone writing them down. At the same time the program pays for proprietary databases, Java runtimes and virtualization licenses whose renewal quotes keep climbing. Most programs can name their largest license contracts. Few can say which open source components they run, who supports them, or which ones have reached end of life.

That gap shows up in three places. The ISSO writes up unsupported components under NIST SP 800-53 SA-22 (the CentOS 7 pattern). A critical vulnerability lands in a common library and the program needs weeks to learn where it is exposed (the Log4j pattern), while CISA Binding Operational Directive 26-04 (June 10, 2026) sets remediation clocks that start at three days with forensic triage for civilian agencies. And a renewal letter or a vendor audit arrives with no inventory to answer it.

This paper is for the people who own those problems: CIOs and CTOs who carry license spend and the agency's code-sharing policy, CISOs and ISSMs who carry supply chain risk, system program managers facing a renewal or an end-of-life date, and the CORs who buy the work. It describes Avalon Technology Services' Open-Source Technologies service, which starts with one engagement:

- **A fixed-fee open-source inventory and license assessment for one program.** One named program boundary, about six weeks. A proprietary license and entitlement inventory with true-up exposure flags; an SBOM-based component inventory for each in-scope system; a support-tier and end-of-life matrix; a list of license obligations routed to agency counsel; a governance gap review against OMB M-16-21 and the SHARE IT Act; and ranked migration candidate memos with level-of-effort estimates. The market band is $45K to $120K firm fixed price.
- **An optional governance sprint.** Three to four weeks to draft and operationalize the program's open source intake and code-sharing policy, priced separately at $25K to $60K.

Section 9 works through an illustrative program with three systems and 2,000 SBOM component entries, which reduce to 1,400 unique components. 9 of 18 platform components have no funded support path, 3 of them past end of life; 84 libraries are unmaintained; 70 license flags go to counsel; and 3 proprietary contracts worth $1.14M a year renew within 18 months. The illustrative assessment fee is $66K.

Avalon inventories, maps and plans. It does not execute migrations inside this engagement, give legal opinions on licenses, or issue or guarantee an ATO. Counsel decides license questions, and the authorizing official decides risk.

Why Programs Cannot Say What They Run

The phrases below come up whenever a program office talks about open source or license cost. Each points to the same missing piece: an inventory that ties components to systems, support and licenses.

What the program says	What it usually means
"Our VMware renewal came back at three times last year's number."	No ranked view of which workloads could move, and at what effort, before the renewal date
"We got a Java audit letter and nobody knows what we're actually running."	No entitlement inventory matched to what is deployed
"We still have CentOS 7 boxes in production and the ISSO keeps writing it up."	No support-tier or end-of-life calendar, so SA-22 findings arrive by audit
"When Log4j hit, it took us three weeks to figure out where we were exposed."	No current SBOM for each system, stored where it can be searched
"Our developers pull packages straight off the internet."	No vetted internal repository and no intake criteria
"Security won't approve anything open source here."	Open source runs anyway, unreviewed; the intake workflow is the fix

Four Misconceptions

- **"Open source means free."** The license may cost nothing; support, patching and migration do not. A component with no funded support path is a cost the program has not booked.
- **"Open source is inherently insecure" or "inherently audited."** Neither. Security depends on maintenance health, provenance and whether the program knows the component is there.

- **"The FAR won't let us use it."** DoD CIO guidance treats open source software as commercial software, and civilian agencies run it in authorized systems every day.
- **"We generated an SBOM once."** An SBOM produced for one build and never refreshed answers yesterday's question. It has to be regenerated as the software changes.

The Policies and the Calendar

Driver	What it says	What it means for this engagement
OMB M-16-21, Federal Source Code Policy (2016)	Reuse of custom-developed code across government and a code inventory published through Code.gov	The governance review checks the program's code inventory and release decisions against it
SHARE IT Act (signed into law)	Government-wide sharing of custom-developed code, with responsibilities for the agency CIO	The review flags policy and metadata gaps; it does not declare the program compliant
OMB M-26-05 (Jan 23, 2026)	Rescinded M-22-18 and M-23-16; agencies set their own risk-based software assurance policies	SBOMs are a contract term the agency may choose, and the CISA attestation form is optional; the assessment gives the agency the inventory to decide
NIST SP 800-218 (SSDF) and SP 800-161 Rev. 1	Secure development practices; supply chain risk management practices	Guidance used to frame the intake criteria and supplier questions, not a mandate
CISA BOD 26-04 (Jun 10, 2026)	Risk-based remediation clocks for known exploited vulnerabilities, from three days with forensic triage to 14 days, 60 days or the next upgrade; replaced BOD 22-01 and BOD 19-02	A current component inventory is what lets a civilian program start the clock on time
NIST SP 800-53 Rev. 5	SA-22, CM-8, CM-10, CM-11, SR-3, SR-4, SR-11, SA-15, SI-2	The control IDs the deliverables give evidence for
Vendor end of support	SQL Server 2016 ended July 14, 2026; Windows Server 2016 ends January 12, 2027	Platform end-of-life dates go into the support matrix next to open source ones

Common triggers: a renewal spike or a vendor audit letter, an end-of-life finding in an assessment, inspector general or GAO review, a critical component vulnerability the program could not scope, gaps in the agency's SHARE IT Act policy or reporting, and fourth-quarter operations and maintenance funds in July through September.

What the Assessment Does

The assessment covers one named program boundary, usually two to four systems. It runs inside the agency's own environment and repositories with self-hosted open source tooling (Syft, Trivy, OWASP Dependency-Track, ScanCode), or with a composition tool the agency already licenses. It adds no license line items, installs nothing permanent and scans nothing until access is approved in writing.

Step	Activities
Kickoff and access	Systems in scope named, license and contract records requested, scanning approval and repository access granted in writing, dependencies dated
License and entitlement inventory	Proprietary contracts, entitlements and renewal dates matched against what is deployed; true-up and audit exposure flagged
Component inventory	SBOMs generated in CycloneDX or SPDX for each in-scope system; platform components and libraries separated
Support and end-of-life matrix	Each platform component assigned a support tier and an end-of-life date; unmaintained libraries listed
License flags and governance review	Copyleft and unknown licenses routed to counsel; intake and code-sharing practice checked against M-16-21 and the SHARE IT Act
Migration candidates and readout	Ranked memos with cost, risk and effort per candidate; briefing to the CIO, CISO, ISSM and program office

Three Support Tiers

Every platform component (operating systems, databases, runtimes, middleware, virtualization) lands in one of three tiers:

- **Commercial subscription:** a vendor support contract the agency buys directly or through its own reseller.
- **Community, with an internal SLA:** no vendor contract, but a named agency team, a patch cadence and a funded escalation path.
- **No funded support path:** nobody is on the hook to fix it. These become SA-22 candidates, and the matrix says whether to subscribe, assign internal support or retire.

"Open source" is not the same as "unsupported". The question for the program is who answers when the component breaks at 2 a.m., and the matrix answers it component by component.

Migration Candidates

Candidates are scored on technical fit, mission risk and total cost of ownership, using the agency's own contract figures. Typical patterns: Oracle or SQL Server to PostgreSQL, commercial Java SE to an OpenJDK build, VMware to a KVM-based platform, a commercial service bus to Apache Kafka or Camel. Each memo states effort, sequencing and the support subscription the target would need. Some workloads should stay proprietary, and the memo says so when the numbers do not close.

Deliverables

Deliverable	Format
License and entitlement inventory with true-up and audit exposure flags	Spreadsheet and short executive brief
SBOMs for in-scope systems	CycloneDX or SPDX JSON, regenerable
Support-tier and end-of-life matrix	Spreadsheet with a maintenance cadence
License-obligation flag list for counsel	Spreadsheet with component, license and system
Governance gap review against M-16-21 and the SHARE IT Act	Short memo
Ranked migration candidate memos	One decision memo per candidate

Where the Engagement Stops

The assessment stops at the memos. Migration engineering is a later, separately scoped purchase, one CLIN per named workload. Gate tuning and pipeline security belong to Avalon's separate DevSecOps service, and building a pipeline belongs to the CI/CD Pipelines service. Portfolio disposition belongs to IT Modernization and workload moves to Cloud Migration. The assessment does not refactor application code, author an SSP or authorization package, run a penetration test, operate the stack or resell subscriptions.

Evidence the ISSM and the CIO Can Use

Control	What the deliverables evidence
SA-22	Unsupported system components: the support matrix names each one and a disposition
CM-8	System component inventory, down to the software components in each SBOM
CM-10, CM-11	Software usage restrictions and user-installed software: license flags and intake criteria
SR-3, SR-4, SR-11	Supply chain controls, provenance and component authenticity
SA-15, SI-2	Development process and flaw remediation, enabled by knowing where a component runs

The accurate statement is narrow. The engagement positions the agency to produce and maintain SBOMs for in-scope systems, implement SA-22, CM-8 and SR-family controls, and work toward its code-sharing policy obligations. It does not constitute, replace or guarantee an authorization to operate, a FedRAMP certification or any software attestation.

Accurate	Not accurate
A component inventory and SBOMs as of the review date	Achieves compliance
License flags routed to agency counsel	Legal clearance of every license
A governance gap review	SHARE IT Act compliance
A disposition for each SA-22 candidate	An ATO milestone
Migration memos built on the agency's numbers	Guaranteed savings

How an Engagement Runs

Phase	Timing	What happens
0: Access	2–4 weeks, often in parallel with contract start	Scanning approval, repository access and contract records; nothing is scanned informally
1: Assessment	About 6 weeks	Inventories, SBOMs, support matrix, license flags, governance review, candidate memos, five-business-day agency review, readout
2: Governance sprint (optional)	3–4 weeks	Intake workflow, code-sharing and release criteria, contribution policy and named roles
Later, separate	8–16 weeks per moderate workload	Migration engineering, one CLIN per named workload

What the Agency Provides

- License, contract and entitlement records for the program, including renewal dates.
- Written approval for composition scanning and read access to repositories and build artifacts. Access approvals routinely take two to four weeks, so they are dated government-furnished dependencies with day-for-day schedule relief.
- One engineering point of contact for about four hours a week, and DBA or system owner time for platform questions.
- A CIO-shop policy owner for the governance review, and a route to agency counsel for license questions.
- A weekly access-blocker review with the COR until all access is in place.

What Is Not Included

Included	Separate work
Migration candidate memos	Migration engineering, priced per named workload
SBOMs and an SCA recommendation	SBOM and SCA stage in an existing pipeline, a $15K–$40K add-on per pipeline
License flags	Legal opinions, which stay with agency counsel
Support-tier matrix	Subscriptions, which the agency buys directly
Control evidence	SSP authoring, the authorization package and the AO's decision
Inventory and planning	Pipeline builds, gate tuning, penetration testing and operations
Unclassified programs	Classified or cleared environments

How Avalon Staffs It

Avalon takes one engagement at a time, works business hours, and works on unclassified programs only. Avalon's founder leads the engagement with a named solution architect and engineer and a fractional project manager, hired or subcontracted and listed in the proposal. 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 and a bounded scope.

Requirement	How it is handled
Architect and engineer	Named personnel whose certifications and investigation level match the agency's requirements, listed in the proposal
Civilian access	Public Trust investigation at the tier the agency requires
Privileged access on DoD systems	Personnel holding the DoD 8140 qualification the program requires, as a condition of the engagement
Tooling and data	Self-hosted open source tools inside the agency boundary; SBOMs and findings stay in agency repositories
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

DoD's Iron Bank and Platform One practices are useful benchmarks for hardened containers, and the intake criteria reference them where the security office recognizes them. Avalon does not operate in those environments.

Pricing and How to Buy

Engagement	Market-norm range	Avalon
Inventory and license assessment, one program, about 6 weeks	$45K–$120K	Firm fixed price; illustrative $66K
Governance sprint, 3–4 weeks	$25K–$60K	Firm fixed price, optional CLIN
SBOM and SCA stage in an existing pipeline	$15K–$40K per pipeline	Firm fixed price per named pipeline
Migration engineering	$30K–$150K+ per moderate workload	Later; firm fixed price per named workload

The assessment, with or without the sprint, sits under the $350,000 simplified acquisition threshold and can be bought as an open-market purchase. 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. Larger 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 licenses or subscriptions.

Fees are non-contingent: there is no share of savings and no performance fee. Prices are fixed against named systems and a dated dependency schedule.

Illustration: One Program, Three Systems

The figures below are a planning illustration for one representative unclassified program. They are not a quote and not a result from any engagement.

Components

System	SBOM component entries
System 1 (case management web application)	640
System 2 (data integration service)	910
System 3 (reporting portal)	450
Total entries	2,000
Unique after 30% overlap	1,400

Library finding	Assumed share	Count
Unmaintained or past end of life	6%	84
Strong copyleft (GPL or AGPL family)	2%	28
Weak copyleft (LGPL, MPL, EPL family)	5%	70
No license detected or ambiguous	3%	42

Strong copyleft and unknown licenses (70 components) go to counsel, because code-sharing decisions make them public questions. Weak copyleft is listed but usually needs no action. The 84 unmaintained libraries join the SA-22 list.

Platform Support Tiers

Tier	Platform components	Past end of life
Commercial subscription	7	0
Community, with internal SLA	2	0
No funded support path	9	3
Total	18	3

Half the platform (9 of 18) has nobody on the hook to fix it, and 3 of those are already past end of life. With the unmaintained libraries, the program carries 87 SA-22 candidates. The matrix gives each a disposition: subscribe, support internally or retire.

Proprietary Renewals

Contract	Months to renewal	Annual value	Inside 18 months
Contract 1	4	$310K	Yes
Contract 2	9	$185K	Yes
Contract 3	14	$640K	Yes
Contract 4	22	$95K	No
Contract 5	30	$420K	No
Contract 6	40	$150K	No

3 of 6 contracts, worth $1.14M a year, renew within 18 months. Those are the first candidates for a migration memo, because a memo only helps if it arrives before the renewal decision. The memo may conclude that a contract should stay.

What the Engagement Costs

Scope	Hours	Rate-band range	Planning fee	Note
Base: 3 systems, 6 weeks	336	$57.1K–$74.3K	$66K	Inside band
A: 2 systems, 4 weeks	224	$38.0K–$49.6K	$45K	Floor applies
B: 5 systems, 8 weeks	448	$76.1K–$99.1K	$88K	Split into two scopes
C: base plus 4-week governance sprint	512	$86.8K–$112.6K	$100K	Inside band

The base case staffs a solution architect at 75% ($180 to $250 an hour), an engineer at 50% ($165 to $195) and a project manager at 15% ($135 to $165, a planning assumption) for six weeks at 40 hours: 336 hours, or $57.1K to $74.3K, with a $66K planning fee at the midpoint. A two-system, four-week scope runs $38.0K to $49.6K, under the $45K floor at the low end, so the fee does not go below $45K. A five-system, eight-week scope stays inside the band at $76.1K to $99.1K but runs past the usual six weeks, so it is better split into two scopes. Adding a four-week governance sprint (architect 50%, compliance specialist 50% at $165 to $195, project manager 10%) brings the total to $86.8K to $112.6K. Every case sits far below the simplified acquisition threshold.

Common Pitfalls

Pitfall	How to avoid it
A free pilot that never becomes a purchase	Price the pilot as an optional CLIN
One migration becomes five	One CLIN per named workload
Governance work drifts into running the program office	End at operationalization plus a defined transition
Scanning before approval	Signed agreement and written approval first; never scan informally
Overselling the result	Inventory, flag and plan; counsel decides licenses and the AO decides risk
A community component in a mission-critical role	Never without a funded support path

Conclusion and Next Step

Using open source is not the decision in front of most programs. They already do. The decision is whether they know which components they run, who supports each one, which licenses carry obligations, and which proprietary renewals are worth challenging before the quote arrives.

The natural first step is the fixed-fee inventory and license assessment: one program, about six weeks, under the simplified acquisition threshold, ending in SBOMs, a support-tier and end-of-life matrix, a license flag list for counsel, a governance gap review and ranked migration memos. To discuss a program, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

SBOM
Software bill of materials: a machine-readable list of the components in a build, in CycloneDX or SPDX format.

Software composition analysis (SCA)
Scanning third-party and open source dependencies for known vulnerabilities and license issues.

Copyleft
A license that requires derivative works to be shared under the same terms; strong (GPL, AGPL) or weak (LGPL, MPL, EPL).

SA-22
NIST SP 800-53 control for unsupported system components.

Support tier
Commercial subscription, community with an internal SLA, or no funded support path.

True-up
A vendor's charge for deployed use beyond the entitlements purchased, usually found in an audit.

OSPO
Open source program office: the roles that own intake, contribution and code-sharing decisions.

M-16-21
OMB's 2016 Federal Source Code Policy, covering reuse and inventory of custom-developed code.

Appendix B: Illustration Assumptions

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

Assumption	Value	Basis
Systems and component entries	3 systems, 2,000 entries, 30% overlap	Planning assumption
Library shares	6% unmaintained; 2% strong copyleft; 5% weak copyleft; 3% unknown	Planning assumption
Platform components	18, of which 9 unsupported and 3 past end of life	Planning assumption
Proprietary contracts	6 contracts, $1.80M a year in total	Planning assumption
Rates	$180–$250 architect; $165–$195 engineer and compliance; $135–$165 PM	KB bands; PM rate assumed
Price check	Base fee $66K	Inside $45K–$120K

Appendix C: References

1. **Office of Management and Budget**, *M-16-21, Federal Source Code Policy (2016)*
   https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf
2. **General Services Administration**, *Code.gov*
   https://code.gov
3. **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
4. **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
5. **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

6. **National Institute of Standards and Technology**, *SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices*
https://csrc.nist.gov/pubs/sp/800/161/r1/final

7. **Cybersecurity and Infrastructure Security Agency**, *Software Bill of Materials (SBOM)*
https://www.cisa.gov/sbom

8. **Cybersecurity and Infrastructure Security Agency**, *Known Exploited Vulnerabilities Catalog*
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

9. **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

10. **Department of Defense CIO**, *DoD Open Source Software FAQ*
https://dodcio.defense.gov/open-source-software-faq/

11. **Microsoft**, *SQL Server 2016 lifecycle*
https://learn.microsoft.com/en-us/lifecycle/products/sql-server-2016

12. **Microsoft**, *Windows Server 2016 lifecycle*
https://learn.microsoft.com/en-us/lifecycle/products/windows-server-2016

13. **OWASP**, *CycloneDX Bill of Materials Standard*
https://cyclonedx.org

14. **Linux Foundation**, *SPDX Specification*
https://spdx.dev

15. **Open Source Security Foundation**, *OpenSSF Scorecard*
https://github.com/ossf/scorecard

16. **Acquisition.gov**, *FAR 15.305, Proposal evaluation*
https://www.acquisition.gov/far/15.305

17. **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/