



Securing Tomorrow's Missions Today.



See It First, Prove It After: Enterprise Monitoring for Federal IT

Enterprise Monitoring: fewer tools, alerts people act on, and logging that fits the agency's M-26-14 plan.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
Why Federal Monitoring Stops Working	3
Why It Concentrates in Government	3
How the Need Sounds	3
What Changed in 2026	4
What the Service Does	5
Alerts People Act On	6
Sizing Ingest Before It Sizes the Bill	6
Evidence and Boundaries	6
How an Engagement Runs	7
What the Agency Provides	8
Scope Avalon Takes On Today	8
Pricing and How to Buy	9
Illustration: Rationalizing a Monitoring Estate	9
Common Pitfalls	11
Conclusion and Next Step	11
Appendices	12
Appendix A: Glossary	12
Appendix B: Illustration Assumptions	12
Appendix C: References	13

Executive Summary

Most federal agencies own more monitoring tools than they can name, and still learn about outages from the help desk. Tools were bought program by program, rarely retired, and partly deployed. Cloud migrations moved workloads out of sight of the operations center that watched the data center. Log retention was sized to a mandate that no longer exists. The result is a monitoring estate that costs more each year and answers the basic questions less well: is everything up, is it performing, and can we prove what happened?

In May 2026, OMB M-26-14 replaced the M-21-31 event-logging tiers with a risk-based model built around continuous event monitoring and threat hunting and investigation objectives. CISA has published its Logging Reference Architecture, and every agency is re-planning its logging against the new memo. That makes this a natural moment to rationalize the monitoring estate rather than add to it.

This paper is written for CIOs and IT operations directors, CISOs and ISSMs, system owners, and the contracting officers who buy the work. It describes Avalon Technology Services' Enterprise Monitoring service in three shapes:

- **A monitoring and logging readiness assessment.** A fixed-price engagement of three to five weeks that inventories tools and coverage, samples alert quality, maps logging against the agency's M-26-14 plan, and delivers a costed roadmap.
- **An implementation or consolidation.** A fixed-price engagement of about 12 to 20 weeks that builds the target monitoring architecture, onboards sources, retires overlapping tools and tunes alerts.
- **A business-hours monitoring retainer.** Optional monthly support for tuning, source onboarding and reporting after the build.

Section 9 works through an illustrative component paying for six overlapping tools. Consolidating to three and resizing retention costs \$280K in engineering and removes about \$492K a year from the run rate, paying back in about 15 months. If tool contracts cannot end for another year, payback stretches to 20 months, which is why renewal dates drive the plan.

Why Federal Monitoring Stops Working

Risk	How it shows up
Mission	Systems fail silently. When the first signal is a help desk ticket, detection is late and restoration starts late.
Compliance	Logging requirements change on policy timelines, not budget timelines. Agencies that never fully met the old tiers now face a new model and new plans.
Cost	Four to eight overlapping products at partial deployment, plus retention volumes sized to rules that no longer apply.
Staffing	Cloud migrations finish without monitoring parity, and the operations team that understood the data center has no equivalent view into cloud workloads.

Why It Concentrates in Government

- **Tools accrete.** Monitoring is bought program by program and procurement by procurement, with no enterprise rationalization step. Retiring a tool is nobody's funded task.
- **Mandates arrive before budgets.** Logging requirements were bolted onto whatever platform existed rather than designed for.
- **One-year money favors point purchases.** O&M funding rewards buying another tool over re-architecting the ones in place.
- **Staff gaps.** Tools get bought but never fully deployed or tuned.

How the Need Sounds

"We find out about outages from the help desk." "My team touches six consoles before coffee." "Everything is red, so nothing is red." "We lost visibility when we moved to the cloud." "The IG dinged us on log retention." "Our log platform bill doubled and we can't say what we get for it." "The SOC keeps asking for logs we don't have." Each of these is this service.

What Changed in 2026

Driver	What it means
OMB M-26-14 (May 2026)	Replaced M-21-31's event-logging tiers with a risk-based model built around continuous event monitoring and threat hunting and investigation objectives, with a maturity model agencies plan against. Agencies are re-planning their logging under it.
CISA Logging Reference Architecture	Published to guide agencies on which logs to collect and how to architect collection for monitoring and investigation. Agency logging plans build on it.
Retention sized to old rules	Many agencies sized storage and licenses to M-21-31's retention periods. A risk-based plan is an opportunity to resize, with the agency's risk decisions written down.
Vendor consolidation	Cisco's acquisition of Splunk, Exabeam's merger with LogRhythm and SolarWinds' move to private ownership have turned routine renewals into architecture decisions.
OpenTelemetry	Open telemetry standards reduce lock-in to proprietary agents and make consolidation easier to plan.

A logging plan that the agency cannot implement, or that its tools cannot report against, is a plan on paper. The work this service does is the engineering underneath the plan.

What the Service Does

Activity	What happens
Readiness assessment	Inventory every monitoring and logging tool (licensed, deployed and shelfware); map telemetry coverage against the asset inventory; sample alert quality; baseline log collection, retention and searchability against the agency's M-26-14 plan; interview operations, ISSO and SOC staff; deliver a prioritized, costed roadmap
Target architecture and rationalization	Decide which platforms stay and which retire; design data flows, agent and collector strategy, ingest sizing with a growth model, retention tiers and integrations with ITSM, notification and the SOC
Implementation	Deploy and configure the chosen platforms, roll out agents and collectors through change control, onboard log sources against an agreed source matrix, and build the pipeline that normalizes, routes and retains data
Operational content	Dashboards for named audiences, alerts with thresholds, owners and escalation paths, service-level objectives for priority services, and runbooks for the most common alerts
Operationalization	Alert tuning cycles, training, documentation and transition to agency operations or to a retainer
Business-hours retainer (optional)	Ongoing tuning, source onboarding, dashboard maintenance and monthly reporting

Delivery is vendor-neutral. Platform choices follow the agency's installed base, the FedRAMP status of any SaaS option and license economics. Avalon resells no licenses; the agency buys them through its own vehicles. Typical platforms include Splunk, Elastic and Microsoft Sentinel for logs; SolarWinds, Zabbix and native AWS CloudWatch or Azure Monitor for infrastructure; Dynatrace or Datadog for application performance; and Prometheus, Grafana and OpenTelemetry pipelines.

Alerts People Act On

An alert nobody acts on trains the operations team to ignore alerts. The assessment samples alerts to measure how many led to action and how many were noise or duplicates. The tuning cycle then raises thresholds, merges duplicates, assigns every alert an owner and an escalation path, and retires alerts that no one would act on. The aim is fewer, better alerts, with silent-failure gaps closed for the services that matter most.

Sizing Ingest Before It Sizes the Bill

Underestimating daily log ingest is the classic monitoring implementation failure: the license bill grows six months after go-live, and nobody planned for it. Every design includes a measured ingest baseline, a growth model and a retention cost table, so the agency sees the cost of each logging decision before it makes it.

Evidence and Boundaries

Control	What the service supports
AU-2, AU-6, AU-11, AU-12	Log source onboarding, review support and retention aligned to the agency's logging plan
CA-7	Continuous monitoring data and dashboards the ISSO can use
SI-4	System monitoring: health, availability and anomaly alerting with documented thresholds
CM-8	Coverage mapped against the asset inventory, with gaps listed

The service produces implementation notes the ISSO can use in the SSP. It does not author the SSP, assess controls or make authorization decisions, and it does not "achieve M-26-14 compliance": the agency's plan and reporting do that.

Included	Separate work
The telemetry pipeline and health and availability alerting	Security detection content, alert triage and threat hunting
Escalating a suspected compromise	Incident response and forensics
Showing what is degrading and where	Fixing network devices and databases
Utilization and consumption telemetry	Cost recovery analysis (FinOps)
Continuous monitoring evidence	The authorization package and decision
Design, sizing and implementation	Platform licenses

How an Engagement Runs

Phase	Typical duration	What happens
0. Kickoff and access	1–2 weeks	Accounts, network access, tool administrator access, asset and tool inventories
1. Assess and baseline	2–4 weeks	Tool and license inventory, coverage map, alert sampling, logging gap analysis, interviews
2. Design	2–3 weeks	Target architecture, consolidation decisions, ingest and retention design, change board approval
3. Implement	4–10 weeks	Pilot enclave first, then phased rollout of agents, sources, pipeline and integrations
4. Operationalize	2–4 weeks	Alert tuning, dashboards, runbooks, training, service-level baselines
5. Transition	1–2 weeks	Configuration and documentation handoff, or start of the retainer

A component-level engagement typically takes 12 to 20 weeks; a single-platform deployment, 8 to 10. The assessment alone takes three to five weeks.

What the Agency Provides

- Accounts and network access by an agreed date. Agency account issuance commonly takes 30 to 60 days and is the most common schedule risk.
- Administrator access to existing tools, and the current asset inventory, or a frank statement that there is not one.
- Change board slots for agent and collector deployment, and firewall changes for collector traffic.
- ISSO review and approval of agents and collectors inside the authorization boundary.
- Named staff for interviews, decisions and knowledge transfer.

The statement of work ties each phase start to these items and includes a clock-stop when access slips, so delays are visible and attributed correctly.

Scope Avalon Takes On Today

Engagement	Position
Readiness assessment	Offered
Component-level implementation, one enclave and one platform family	One engagement at a time
Enterprise multi-tool consolidation at a large agency	As a subcontractor or teamed, not as a solo prime
Round-the-clock monitoring or operations center staffing	Not offered; business-hours retainer only
Classified environments	Not offered

Each engagement is staffed with named personnel whose platform certifications and investigation level match the agency's requirements, listed in the proposal. Avalon cites no certification, clearance, vendor partnership or past engagement that is not current and verifiable, and it has no prior federal contracts under this service.

Pricing and How to Buy

Engagement	Market-norm range
Readiness assessment	\$25K–\$75K at component scope (Avalon: \$25K–\$45K fixed price)
Implementation or consolidation, component level	\$75K–\$300K fixed price
Enterprise multi-tool consolidation	\$300K–\$1.5M
Business-hours retainer	\$8K–\$25K a month
Monitoring parity inside a migration	\$20K–\$60K as a line item

Implementations are priced as fixed price against a locked source matrix, with unit prices for additional sources. Every implementation quote follows an assessment, because quoting without a measured ingest baseline is how sizing errors happen.

The assessment and most component-level implementations fit under the \$350,000 simplified acquisition threshold, so they can be bought as open-market purchases with one-year O&M funds. Larger work can be subcontracted to Avalon by a prime that already holds the agency's vehicle. Avalon does not hold a GSA Schedule or a governmentwide contract today.

Illustration: Rationalizing a Monitoring Estate

The figures below are a planning illustration for one agency component, not a quote and not a result from any engagement. Licenses and storage are the agency's costs under either path.

Current tool	Annual cost	Plan
Log management platform A	\$380K	Keep
Log management platform B	\$140K	Retire at renewal, month 10
Infrastructure monitoring	\$85K	Keep
Application performance monitoring	\$120K	Keep
Network monitoring	\$55K	Retire at renewal, month 7
Legacy network management system	\$35K	Retire at renewal, month 4

Today the component spends about \$815K a year on these tools, \$160K on log retention sized to the old M-21-31 rules, and 2.0 full-time equivalents keeping six consoles, agents and integrations working. The plan keeps three tools, filters low-value log sources to cut log platform cost by 20%, resizes retention to the agency's M-26-14 plan (\$105K a year), and reduces maintenance effort to 1.25 FTE after consolidation. Engineering is a \$40K assessment and a \$240K implementation.

Scenario	One-time cost	Annual saving at run rate	3-year net	Payback
Base case	\$280K	\$492K	\$872K	15 months
Renewals locked one more year	\$280K	\$492K	\$642K	20 months
Smaller ingest cut (10%)	\$280K	\$454K	\$777K	16 months
Implementation at top of band (\$300K)	\$340K	\$492K	\$812K	17 months

In the base case, the component saves about \$872K net over three years. Savings arrive only as each retired tool's contract ends, so renewal dates set the pace. If those contracts cannot end for another year, payback moves from 15 to 20 months. That is why the assessment lists every renewal date and why the plan starts with the tools whose contracts end first.

A smaller ingest cut (10% instead of 20%) or an implementation at the top of the price band moves payback by only a month or two. The retention resize depends on the agency's own risk decisions under M-26-14; the plan documents those decisions so the storage change is defensible.

Common Pitfalls

Pitfall	How to avoid it
"Monitor everything"	A locked source matrix in the contract; additions priced per source
Security detection work creeping in	Detection content and alert triage named as separate work
A dashboard for every stakeholder	A dashboard count per audience tier, with a change path
Ingest sizing errors	A measured baseline, growth model and retention cost table in every design
Compliance overselling	Describe evidence and implementation, never "M-26-14 compliant" or "ATO-ready"

Conclusion and Next Step

Agencies do not need more monitoring tools. They need fewer, better-configured ones, alerts that someone acts on, and logging that matches the plan they now owe under M-26-14. The re-planning cycle is the moment to make that change, because the logging decisions and the tool decisions are the same decisions.

The natural first step is a readiness assessment: three to five weeks, a fixed price well under the simplified acquisition threshold, and a costed roadmap that lists every tool, every renewal date and every logging gap. To discuss an assessment, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

Alert quality

The share of alerts that lead to action, as opposed to noise or duplicates.

Ingest

The volume of log data a platform receives each day; it drives license and storage cost.

LRA

CISA's Logging Reference Architecture, guidance for agency logging under M-26-14.

M-26-14

OMB memorandum of May 2026 on agency logging and network visibility. It replaced M-21-31 with a risk-based logging model.

OpenTelemetry

An open standard for collecting metrics, logs and traces without proprietary agents.

Source matrix

The agreed list of log sources to onboard, with owners and retention.

SLO

Service-level objective: a measurable target for a service's availability or performance.

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
Tools	6 today; 3 kept	Planning assumption
Retired tool savings	From each tool's renewal month (4, 7 and 10)	Contracts end at renewal
Log platform ingest cut	20% from month 6 (10% alternate)	Filtering low-value sources
Retention storage	\$160K to \$105K a year from month 6	Resized to the agency's M-26-14 plan
Maintenance effort	2.0 to 1.25 FTE from month 9 at \$175K each	Fewer consoles and integrations
Engineering	\$40K assessment; \$240K implementation (\$300K alternate)	Inside the bands in Section 8
Renewal lock	12 more months (alternate)	Contracts that cannot end early
Horizon	3 years, undiscounted	Planning assumption

Appendix C: References

1. **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>
2. **Cybersecurity and Infrastructure Security Agency**, *Logging Reference Architecture*
<https://www.cisa.gov/resources-tools/resources/logging-reference-architecture>
3. **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>

4. **National Institute of Standards and Technology**, *SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations*
<https://csrc.nist.gov/pubs/sp/800/137/final>
5. **National Institute of Standards and Technology**, *SP 800-92 Rev. 1 (draft), Cybersecurity Log Management Planning Guide*
<https://csrc.nist.gov/pubs/sp/800/92/r1/ipd>
6. **OpenTelemetry**, *OpenTelemetry documentation*
<https://opentelemetry.io/docs/>
7. **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/>