AVALON
TECHNOLOGY SERVICES

Securing Tomorrow's Missions Today.

★★★
2026

From Stale Ledger to Defensible Record: POA&M Cleanup for Agency ISSMs

Plan of Action & Milestones (POA&M): current, complete, evidence-backed records and a remediation cadence the government team can keep.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary **2**

Why POA&M Ledgers Go Stale **3**
Why It Concentrates in Government 3
How the Need Sounds 3

What Changed in 2025 and 2026 **4**

What the Service Does **5**
A Milestone an AO Can Believe 5
Reconciling BOD 26-04 Clocks 6

Where the Requirement Lives **7**

How an Engagement Runs **8**
What the Agency Provides 9
What Is Not Included 10

How Avalon Staffs It **10**

Pricing and How to Buy **11**

Illustration: Rationalizing One Enclave's Ledger **12**

Common Pitfalls **14**

Conclusion and Next Step **15**

Appendices **15**
Appendix A: Glossary 15
Appendix B: Illustration Assumptions 16
Appendix C: References 16

Executive Summary

Every system in an agency's FISMA inventory carries a plan of action and milestones: the record of each known weakness, the planned fix, the resources behind it, the interim milestones and the scheduled completion date. It is one of three documents in every authorization package, alongside the system security plan and the assessment report. It is also the one most likely to be stale.

The pattern is familiar to any ISSM. Assessments, monthly scans, STIG checks, penetration tests, CISA directives and IG audits all feed the same ledger, while ISSO positions sit vacant or cover many systems each. Items get duplicated, milestone dates get rolled forward every quarter, closure evidence never gets written, and legacy weaknesses that will never be fixed economically sit open without the risk decision they need. When an Authorizing Official faces a reauthorization on a system with hundreds of aged, unresourced items, there is little in the record to rely on.

This paper is written for ISSMs and ISSOs, system owners, CISOs and the CORs who buy the work. It describes Avalon Technology Services' POA&M service, delivered in two shapes:

- **A cleanup sprint.** A fixed-price engagement of 8 to 12 weeks for one system or enclave that baselines the ledger, rationalizes it, rebuilds milestones against real resources, packages closure evidence for items already fixed, drafts risk decision memos, and hands the government team a cadence it can keep.
- **A monthly retainer.** Ongoing POA&M management after the sprint: working sessions, status updates, new findings reconciled into the ledger and a monthly status brief.

Section 9 works through an illustrative sprint for one enclave with 600 raw open items. Under stated assumptions, rationalization yields about 420 defensible items for roughly 452 analyst hours and 96 lead hours, a fixed price near $74K, or about $176 per rationalized item. It also shows what slow account provisioning and a different duplicate rate do to that plan.

The work runs inside the agency's own eMASS, CSAM or Xacta instance. Avalon drafts; the government decides.

Why POA&M Ledgers Go Stale

Risk	How it shows up
Authorization	An AO facing a renewal decision on a system with hundreds of aged, unresourced open items has little basis for a decision. Open items do not by themselves block an authorization; unmanaged ones make the decision hard to defend.
Audit	Weak remediation programs and stale POA&Ms are perennial findings in annual IG FISMA evaluations and GAO reviews, and those findings roll up to the CISO and the agency head.
Reporting	POA&M timeliness and data quality feed the CIO FISMA metrics agencies submit quarterly through CyberScope. Bad records become visible above the agency.
Security	A finding that sits open and untracked for 400 days is an unmitigated weakness, not a documented one.

Why It Concentrates in Government

- **Findings arrive faster than staff can process them.** Assessments, scans, STIG checks, penetration tests and directives all land in one ledger, often kept by one ISSO across several systems.
- **Legacy weaknesses need paperwork, not patches.** Some findings cannot be fixed economically on an aging platform. They need a documented risk decision, and nobody has time to write it.
- **Tool friction.** eMASS and CSAM entries are tedious to maintain, and scan results often never make it into the POA&M at all.
- **Incentives.** Support contractors are often paid to maintain the ledger, not to make it smaller or more accurate, so backlogs grow quietly until an IG or an expiring ATO forces the issue.

How the Need Sounds

"Our POA&Ms are all red." "We just roll the dates every quarter." "Nobody writes closure evidence." "Scan findings never actually make it into the POA&M." "The AO said clean it

up or he won't sign." "We inherited nine hundred open items from the last contractor." Each of these is this service. "We don't know our gaps" is an assessment need instead.

What Changed in 2025 and 2026

Date	Event	What it means for the POA&M
September 24, 2025	DoD announces the Cybersecurity Risk Management Construct (CSRMC)	RMF, DoDI 8510.01 and eMASS remain in use; DoD POA&Ms still live in eMASS
October 1, 2025	Simplified acquisition threshold rises to $350,000	A cleanup sprint, and a year of retainer, fit an open-market buy
February 6, 2026	CISA BOD 26-02 on end-of-support edge devices	Inventory in 3 months, decommission in 12, replace in 18; each device left in place needs a tracked plan
May 2026	OMB M-26-14 replaced M-21-31 with a risk-based logging model	Logging gaps found against the new model become POA&M entries
June 10, 2026	CISA BOD 26-04 replaces BOD 22-01 and BOD 19-02	Risk-based clocks of 3 days (with forensic triage), 14 days, 60 days and next upgrade; policy immediately, processes within 60 days, full timelines within about 180 days
June 25, 2026	FedRAMP Consolidated Rules published	Cloud offerings become FedRAMP Certified in classes A to D; the change covers the provider's offering, not the agency's own systems
July 13, 2026	CMMC Phase 2 suspended	Phase 1 self-assessment and NIST SP 800-171 plans of action remain

None of the 2026 changes removes the agency's own POA&M obligation. FedRAMP's move toward machine-readable, continuous evidence changes how cloud providers report their weaknesses. Agency FISMA systems still need a plan of action for every

open weakness, and agencies that sponsor or reuse cloud services still need to track the customer-responsibility items that sit on their side.

What the Service Does

The difference between this service and an undifferentiated "ISSO support" line is that the work is scoped as five named activities with defined outputs, not seat time.

Activity	What it covers
POA&M development	Raw findings (assessment reports, ACAS, Nessus or Qualys scan output, STIG failures, penetration test reports, IG and GAO findings, incident corrective actions) turned into complete entries: weakness, source, severity, affected assets, responsible party, resources, interim milestones and a completion date that reflects an actual plan
Backlog rationalization	Duplicates removed and overlapping items consolidated; severity re-scored against CVSS, the CISA Known Exploited Vulnerabilities catalog and agency risk criteria; risk decision candidates identified; milestones re-baselined against real resource availability
Remediation coordination cadence	Weekly or biweekly working sessions and monthly status reporting that chase owners, update status, escalate blocked items and reconcile new scan findings into the ledger
Closure evidence engineering	Per-item packages (configuration artifacts, before and after scan results, screenshots, change records, sign-offs) formatted the way the agency's assessor and AO expect
Risk decision documentation	Draft risk acceptance memos, deviation and waiver requests, and operational justifications for the government's decision-makers to adjudicate

A Milestone an AO Can Believe

A milestone is believable when it names an owner, the resources committed, the dependency it waits on and a date the owner agreed to. "Remediate by Q3" is a placeholder. "Apply vendor patch to 14 hosts in the March change window, owner:

platform team lead, dependency: vendor fix release, evidence: rescan within 7 days" is a plan. Re-baselining a milestone is honest only when the new date is tied to a resource and the original detection date is kept; the age of the weakness never resets.

Reconciling BOD 26-04 Clocks

For civilian agencies, BOD 26-04 sets risk-based remediation clocks. A POA&M milestone that says one thing while the directive says another is a contradiction an auditor will find. During rationalization, each item tied to a directive-covered vulnerability is checked against the applicable clock, and milestone dates that conflict with it are flagged for the system owner to fix or to route through the agency's documented process. The service does not decide which tier applies to an agency's assets; it makes the ledger consistent with the decisions the agency has made.

Where the Requirement Lives

Authority	Requirement	What the service supports
FISMA (44 U.S.C. § 3554) and OMB Circular A-130	A process for planning, implementing and documenting remedial action	A documented process and current records
OMB M-02-01 and annual FISMA reporting	POA&M preparation and quarterly CIO metrics through CyberScope	Timely, accurate, metric-ready records
NIST SP 800-53 Rev. 5	CA-5 (system POA&M) and PM-4 (organization-wide process), fed by CA-2, CA-7, RA-5, RA-7 and SI-2	Implementation evidence for CA-5 and PM-4
NIST SP 800-37 Rev. 2	Assess step Task A-6 produces the POA&M; Monitor step tasks keep it current	A package element the AO can rely on through ongoing authorization
NIST SP 800-171 (3.12.2 in Rev. 2; 03.12.02 in Rev. 3)	Plans of action for unimplemented CUI requirements; open items affect the SPRS score	Defensible plans of action for contractor systems
CMMC (32 CFR Part 170)	Level 1 permits no plans of action; Level 2 permits a limited set with a 180-day closeout	Closeout discipline; Phase 2 is suspended, the 800-171 obligation stands
CISA BOD 26-04	Risk-based remediation clocks for civilian agencies	Milestone dates consistent with directive clocks

Where machine-readable exchange is in play, records can be structured to the NIST OSCAL POA&M model. The POA&M is a mandatory component of the authorization package, not a prerequisite to it and not an add-on.

Accurate	Not accurate
Current, complete, evidence-backed POA&M records and a functioning remediation cadence that strengthen the authorization package and FISMA reporting posture	Closes the findings, or a closure count
Closure evidence packaged for the assessor's validation	Validated or closed items
Draft risk decision memos for the AO	Accepted risk
Support to the authorization package	Achieves or preserves the ATO, or determines an IG rating

How an Engagement Runs

Phase	Weeks	What happens
Intake and baseline	1–2	Account provisioning, ledger export, data-quality and aging analysis, baseline report
Rationalize and re-baseline	3–6	Deduplicate and consolidate, re-score, identify risk decision candidates, rebuild milestones against real resources
Cadence and closure	5–10	Working-session rhythm stood up; closure evidence packages for validation-ready items
Handoff	10–12	SOP delivered, government team trained on the cadence, exit brief to the ISSM and CISO

A single enclave with a few hundred items fits the 8-to-12-week sprint. A portfolio of 10 to 15 systems runs four to six months. After a sprint, ongoing management is a monthly retainer, not another project.

Deliverable	Format
Baseline assessment: counts, aging, data-quality defects, duplicate rate, risk concentrations	Short report (PDF) and briefing deck
Rationalized POA&M of record	Native entries in eMASS, CSAM or Xacta, or the governing workbook template (XLSX)
Risk-ranked remediation priority matrix	XLSX, sortable by severity, KEV status, effort and authorization impact
Closure evidence packages	Per-item artifact folders with a standard cover sheet
Draft risk acceptance and deviation memos	Word, formatted for agency signature routing
POA&M management SOP and cadence calendar	Word, left with the government team
Monthly status brief in CIO-metric language	One-page PDF or short deck

What the Agency Provides

- Sponsored eMASS, CSAM or Xacta accounts and CAC issuance. These take two to six weeks or more, so paperwork starts at award and the access date is a named government milestone in the schedule.
- System-owner participation in milestone and closure decisions, with the named participants and their expected hours written into the SOW.
- Scan output, prior assessment reports, IG or GAO findings and the current SSP for reference.
- Key dates (assessments, authorization decisions, reporting deadlines) in the integrated schedule.
- Findings data handled inside the government environment. The work is performed there, not on contractor systems.

What Is Not Included

Included	Separate work
Building and maintaining POA&M records from findings	Performing the assessment or scan that produces findings
Milestone engineering, resourcing and scheduling	Executing the technical fixes
Preparing closure evidence packages	Validating closure, which belongs to the assessor and AO
Drafting risk acceptance and deviation documents	Accepting risk, which is the AO's decision alone
Record hygiene inside the existing tool instance	Standing up, licensing or migrating the GRC platform
Pointer-level SSP updates where a POA&M item changes a statement	Writing or rewriting the SSP

If the agency also intends to buy remediation work that the POA&M analysis scopes, a potential organizational conflict of interest exists. Avalon discloses it in the proposal and proposes mitigation, such as firewalled recommendations or recusal from directly scoped follow-on work.

How Avalon Staffs It

Avalon takes one engagement at a time: one cleanup sprint, or one bundled POA&M workstream inside a larger authorization engagement, on unclassified systems. Avalon has no prior federal engagements under this service. Each engagement is staffed with named personnel whose certifications and investigation level match the agency's requirements, and those personnel are listed in the proposal.

Requirement	How it is handled
Team shape	One GRC/POA&M analyst at 0.5 to 1.0 FTE, a senior compliance lead at about 0.2 FTE, fractional project management
DoD ISSO-support roles	Personnel qualified under DoD 8140 for the 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
CUI handling	All work performed inside the government environment; findings data does not move to contractor systems
Classification	Unclassified systems only

The mitigation for that is structural: a small fixed-price scope that caps the agency's exposure, the method and deliverable formats shown before award, and a handoff SOP so the agency depends less on any contractor afterward, Avalon included.

Pricing and How to Buy

Shape	Market-norm range
Cleanup sprint (one system or enclave, 8–12 weeks)	$35K–$90K, firm fixed price
Bundled workstream inside an A&A engagement	$15K–$40K labeled line inside a $100K–$250K engagement
Portfolio rationalization (5–15 systems, 4–6 months)	$100K–$250K
Monthly retainer after a sprint	$6K–$18K a month

Sprints are priced fixed against a tight scope statement. Ongoing management is priced as time and materials or fixed-price level of effort. Nothing is priced on closure counts,

because closure depends on fix resources, assessor judgment and AO decisions the service does not control.

A sprint, and a sprint plus a year of retainer across most of the range, fit under the $350,000 simplified acquisition threshold, so they can be bought as open-market purchases with one-year O&M 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. POA&M work inside a larger authorization or support task order can be subcontracted to Avalon by the prime. Avalon does not hold a GSA Schedule or a governmentwide contract today.

Illustration: Rationalizing One Enclave's Ledger

The figures below are a planning illustration for one enclave, not a quote and not a result from any engagement. Every input is a stated assumption in Appendix B.

The enclave's ledger holds 600 raw open items. At intake, 330 are past their scheduled completion date and only 150 have a named owner and a resourced milestone. The assumptions: 30% of raw items are duplicates or consolidate into another item, 15% of what remains is already fixed and needs only closure evidence, and 8% are candidates for a risk decision memo.

Ledger outcome	**Items**
Raw open items at intake	600
Removed as duplicates or consolidated	180
Rationalized items of record	420
Validation-ready: closure evidence packaged for the assessor	63
Risk decision candidates: memo drafted for the AO	34
Open items with rebuilt, resourced milestones	357

Work	Analyst hours
Intake and baseline	48
Deduplicate, consolidate and re-score	90
Rebuild milestones with owners	107
Closure evidence packages	79
Draft risk decision memos	68
Working sessions and status, weeks 5–10	36
SOP, training and exit brief	24
Total analyst hours	452

Add 96 senior lead hours, at $125 an hour for the analyst and $185 for the lead, and the effort comes to about $74.2K, a fixed price near $74K. That is inside the $35K–$90K band and works out to about $176 per rationalized item, or $123 per raw item. The analyst runs at about 0.94 FTE over 12 weeks.

Scenario	Items	Analyst hours	Price	Per item	Award to done
Base case (access in 2 weeks, 30% duplicates)	420	452	$74K	$176	12 weeks
Slow access (accounts and CAC in 6 weeks)	420	452	$74K	$176	16 weeks
Cleaner ledger (15% duplicates)	510	505	$81K	$159	12 weeks
Messier ledger (45% duplicates)	330	396	$67K	$203	12 weeks

Slow access. If accounts and CAC take six weeks instead of two, the work is unchanged but the agency waits 16 weeks from award instead of 12. If an authorization

decision or the end of the period of performance is fixed, those four weeks come out of the cadence and closure phase. That is why the access date belongs in the SOW as a government milestone and the period of performance should run from access, not award.

Duplicate rate. The duplicate rate cuts the other way from intuition. A cleaner ledger with 15% duplicates leaves 510 real items, more milestones to rebuild and more evidence to package: about 505 analyst hours, slightly more than one full-time analyst over twelve weeks, and a price near $81K. A messier ledger with 45% duplicates leaves 330 items and a price near $67K, but costs more per item that remains ($203). The baseline measures the real rate in the first two weeks, and a change in scope beyond the planned range goes through a priced change order.

Aging is reported honestly. After the sprint, the 357 open items carry milestones tied to a named owner and resource, against 150 at intake. Their original detection dates are unchanged, because re-baselining changes the plan, not the history.

Common Pitfalls

Pitfall	How to avoid it
Management drifts into execution ("while you're in there, just fix it")	An SOW statement that fixes are out of scope and priced separately
Milestone work drifts into SSP rewriting	SSP work capped at pointer-level updates; anything more is separate
"Manage the POA&M" becomes "attend every meeting"	The cadence (which meetings, how often, which reports) defined in the SOW
Schedule starts at award, not at access	Account and CAC provisioning as a government milestone, reported from week one
System owners unavailable for milestone decisions	Named government participants and expected hours in the SOW
Rolling dates without resources	Every re-baselined date tied to an owner and resource; detection dates never reset
Bundled POA&M work given away	A labeled line at the same rates as the rest of the authorization work

Conclusion and Next Step

The POA&M is what the AO and the IG actually read. A stale ledger turns technical risk into audit findings and a hard authorization decision; a current one gives the AO a record to rely on, whatever the open count. AOs routinely authorize systems that carry open, well-managed POA&M items. What they cannot work with is a ledger that does not reflect reality.

The natural first step is a cleanup sprint: one system or enclave, a fixed price under the simplified acquisition threshold, a written baseline in the first two weeks, and a handoff SOP the government team keeps. To discuss a sprint, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

AO
Authorizing Official: the senior official who accepts risk and makes the authorization decision.

CA-5 / PM-4
NIST SP 800-53 controls for the system-level plan of action and milestones and the organization-wide POA&M process.

CSAM
Cyber Security Assessment and Management: a GRC tool used across much of the civilian government.

eMASS
Enterprise Mission Assurance Support Service: DoD's system of record for RMF packages and POA&Ms.

KEV
CISA's Known Exploited Vulnerabilities catalog.

OSCAL
NIST's Open Security Controls Assessment Language, which includes a machine-readable POA&M model.

POA&M
Plan of action and milestones: the record of each known weakness and the plan to correct it.

SCA
Security control assessor: the party that assesses controls and validates closures, independent of the people who do the work.

Appendix B: Illustration Assumptions

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

Assumption	Value	Basis
Raw open items	600	Planning assumption
Duplicate or consolidation rate	30% (15% and 45% alternates)	Planning assumption; measured at baseline
Validation-ready share	15% of rationalized items	Planning assumption
Risk decision candidates	8% of rationalized items	Planning assumption
State at intake	55% past due; 25% resourced	Planning assumption
Effort per item	Baseline 24 h plus 0.04 h per raw item; rationalize 0.15 h per raw item; milestones 0.3 h; evidence 1.25 h; memo 2.0 h	Planning assumption
Cadence and handoff	6 h a week for 6 weeks; 24 h handoff	Planning assumption
Rates	Analyst $125 an hour; lead $185 an hour for 96 h	Inside $95–$150 and $150–$210 market norms
Access lead time	2 weeks (6 alternate)	Government-furnished

Appendix C: References

1. **U.S. Code**, *44 U.S.C. § 3554, Federal agency responsibilities* https://www.law.cornell.edu/uscode/text/44/3554

2. **Office of Management and Budget**, *Circular A-130, Managing Information as a Strategic Resource*
https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/circulars/A130/a130revised.pdf
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 800-37 Rev. 2, Risk Management Framework for Information Systems and Organizations*
https://csrc.nist.gov/pubs/sp/800/37/r2/final
5. **National Institute of Standards and Technology**, *SP 800-171 Rev. 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
https://csrc.nist.gov/pubs/sp/800/171/r3/final
6. **National Institute of Standards and Technology**, *Open Security Controls Assessment Language (OSCAL)*
https://pages.nist.gov/OSCAL/
7. **Cybersecurity and Infrastructure Security Agency**, *Known Exploited Vulnerabilities Catalog*
https://www.cisa.gov/known-exploited-vulnerabilities-catalog
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. **Electronic Code of Federal Regulations**, *32 CFR Part 170, Cybersecurity Maturity Model Certification Program*
https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170
10. **FedRAMP**, *Federal Risk and Authorization Management Program*
https://www.fedramp.gov/
11. **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/