



Securing Tomorrow's Missions Today.



From Finding to Fixed: Remediation and Patch Management Under BOD 26-04

Remediation & Patch Management: backlogs closed in tested waves, unpatchable systems engineered around, and proof of every fix.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
Why Backlogs Grow	3
What Triggers the Work	3
How the Need Sounds	4
The New Clocks: BOD 26-04, BOD 26-02 and FedRAMP	4
What a Remediation Engagement Does	5
Test Before You Deploy: Ring, Change Board, Rollback	6
When There Is No Patch: Mitigation Engineering	7
Proof of Closure	7
Two Delivery Modes	8
Mode A: Remediation Sprint	8
Mode B: Managed Patch Operation	9
The Avalon Team	9
What the Agency Provides	9
What the Service Supports, and What It Does Not	10
What the Service Does Not Include	11
An Illustrative Sprint	11
When the Assumptions Change	12
Pricing and Contracting	13
Risks and How the SOW Contains Them	14
Conclusion and Next Step	14
Appendices	15
Appendix A: Glossary	15
Appendix B: Control Map	16
Appendix C: Illustration Assumptions	16
Appendix D: References	17

Executive Summary

Federal agencies are better at finding security flaws than fixing them. Two decades of investment built scanning, dashboards and enterprise licenses that tell an agency exactly how many findings are open. Far less went into the labor that closes them. The result is a backlog that grows faster than the operations staff can work it, and POA&M items that age until an Inspector General or an Authorizing Official notices.

In June 2026 the gap got a deadline. CISA's Binding Operational Directive 26-04 replaced the flat KEV timeline with remediation clocks set by four questions about each vulnerability. The shortest clock is three days, with forensic triage to check whether an attacker already got in. Earlier in the year, BOD 26-02 set 12- and 18-month deadlines to retire end-of-support edge devices, and FedRAMP's new vulnerability detection and reporting rules become mandatory on December 7, 2026.

This paper is written for ISSMs and ISSOs, CISOs, system owners and operations managers, and the contracting officers who buy the work. It describes Avalon Technology Services' Remediation & Patch Management service, which is the fix stage of a find, fix and prove pipeline. It comes in two forms:

- **A remediation sprint.** A fixed-price engagement of 8 to 16 weeks that burns down a frozen backlog in tested waves and returns proof that each fix worked.
- **A managed patch operation.** A monthly cycle, with an emergency lane for the shortest BOD 26-04 clocks, that keeps the backlog from growing back.

Both run on the agency's own deployment and scanning tools. Section 10 walks through an illustrative entry sprint for one system boundary: 1,200 raw findings deduplicated to 480, closed in weekly waves in about 13 weeks at a fixed price of \$75K. The same section shows what happens when the change board slows down.

Why Backlogs Grow

Cause	How it shows up
Visibility was funded; labor was not	Agencies can report exactly how many findings are open. Far fewer can staff the closure rate those findings require.
Legacy and end-of-support systems	Part of every backlog cannot simply be patched, because the vendor no longer ships fixes or the mission system cannot take them.
Change-control friction	Change advisory boards, scarce maintenance windows and ATO-driven configuration management slow deployment far below the tempo new directives demand.
Fragmented ownership	The ISSO who owns the POA&M, the system owner who holds the ATO and the contractor who touches the servers often sit in three organizations. Findings age in the seams.
Patches that broke things	One bad patch makes system owners refuse the next. Untested deployment creates the resistance that slows every later fix.
Budget mismatch	Remediation labor is bought with annual O&M money, while vulnerability volume arrives continuously and spikes without warning.

What Triggers the Work

- BOD 26-04 clocks, policy-update requirements and implementation milestones.
- An IG or GAO finding on patch or vulnerability management, especially a repeat one.
- An ATO renewal blocked or conditioned on aging POA&M items.
- A DoD Cyber Operational Readiness Assessment (CORA) on the calendar.
- Known exploited vulnerabilities visibly past due on the agency's CDM dashboard.
- End-of-life waves: residual Windows 10 fleets and BOD 26-02 edge devices.
- Year-end O&M funds meeting an unclosed backlog.

How the Need Sounds

"Our POA&M keeps growing." "We can't meet the three-day clock." "We have the scan data but nobody to work it." "Our contractor deploys patches but nothing ever closes." "We're afraid patching will take down the mission application." "Half of it can't be patched anyway." Each of these is this service. If the agency does not yet know what is vulnerable, an assessment comes first.

The New Clocks: BOD 26-04, BOD 26-02 and FedRAMP

Three 2026 changes turned a chronic backlog into a dated obligation.

Requirement	What it sets	Who it binds
CISA BOD 26-04, Prioritizing Security Updates Based on Risk (June 10, 2026)	Remediation clocks from four inputs: public exposure, KEV status, automatable exploitation and technical impact. Three days with forensic triage for KEV-listed flaws that yield total control; then 14 days, 60 days or the next upgrade. Replaced BOD 22-01 and BOD 19-02. Policy updates immediately, process updates within 60 days, full timelines within about 180 days.	Federal civilian agencies; not national security systems
CISA BOD 26-02, Mitigating Risk from End-of-Support Edge Devices (February 6, 2026)	Inventory listed edge devices within 3 months; decommission devices already past end of support within 12 months; replace all identified devices within 18 months; continuous discovery within 24 months.	Federal civilian agencies
FedRAMP vulnerability detection and response, and evaluation and reporting rules	Mandatory from December 7, 2026, replacing legacy monthly-scan continuous monitoring with continuous evaluation aligned to the new risk model.	Cloud service providers and the agencies that rely on them

DoD components are not bound by BOD 26-04, but many track it as practice, and CORA scores remediation discipline directly. For DoD systems, STIG deviations and ACAS findings carry the same operational pressure.

The shortest clock changes the work itself, not only its pace. Patching a flaw an attacker has already used does not remove the attacker. For top-tier findings, the remediation has to include a check for prior compromise, with evidence collected before the patch overwrites it.

What a Remediation Engagement Does

The difference between this service and a generic patching line item is that it delivers a closure pipeline, not just deployment labor.

#	Activity	What happens
1	Findings intake and normalization	Ingest scan exports, penetration test reports, IG and GAO findings, assessment results and open POA&M items, and normalize them into one deduplicated backlog mapped to assets and owners
2	Risk-based prioritization	Assign each finding its BOD 26-04 clock from the four inputs, supplemented by EPSS exploit-prediction scores and mission context. CVSS is supporting context only.
3	Patch engineering and deployment	Acquire and test vendor updates in a test ring, package them for the change board, deploy in approved windows with the agency's own tools, and keep a rollback plan for every wave
4	Configuration remediation	Close STIG and CIS Benchmark deviations, weak protocols and ciphers, unnecessary services, and policy settings, verified with SCAP and STIG tooling
5	Mitigation engineering	Design compensating controls where no patch exists or none can be applied, with a residual-risk statement for the AO
6	Forensic triage coordination	For top-tier findings, coordinate the check for prior compromise; confirmed compromise escalates to incident response

#	Activity	What happens
7	Validation and evidence	Rescan with the same scanner and policy as the baseline, and assemble a closure evidence package for each finding
8	Reporting and metrics	Weekly wave status in sprints; monthly metrics in managed mode, including clock compliance, aging and an agency-attributable delay log
9	Patch management procedure (optional)	Write or refresh the agency's patch and flaw-remediation procedure to NIST SP 800-40 Rev. 4 and BOD 26-04 policy requirements

Deployment runs on whatever the agency already owns: Microsoft Configuration Manager, Intune or WSUS, Tanium, BigFix, Ansible for Linux fleets, and AWS Systems Manager or Azure Update Manager for cloud workloads. Validation uses the agency's scanner, typically Tenable (ACAS in DoD), Qualys or Rapid7. No new platform is required, and none is sold.

Test Before You Deploy: Ring, Change Board, Rollback

The quickest way to stop an agency from patching is to break a mission application with an untested patch. System owners who have been burned refuse the next wave, and the backlog grows. Operational safety is therefore a deliverable, not a disclaimer.

1. **Test ring.** Each update is first applied to a designated test group or pre-production environment for its platform. Where none exists, a pilot ring of production systems is named in writing.
2. **Change board.** Each wave goes to the agency's change advisory board as a complete package: scope, affected systems, test results, deployment window and rollback plan.
3. **Phased deployment.** Waves are grouped by platform and fix type and deployed in approved windows, starting with the least critical systems in each group.
4. **Rollback.** Every wave has a written rollback runbook and a defined response time if a deployment causes a problem.
5. **Validation.** A rescan with the baseline scanner and policy confirms each fix before the finding is counted as closed.

Top-tier BOD 26-04 findings cannot wait for the regular wave cycle. They go through a defined emergency lane with a compressed test step, an expedited change approval agreed with the agency in advance, and the forensic triage check.

When There Is No Patch: Mitigation Engineering

Every federal backlog includes findings that cannot be patched: end-of-support software, frozen mission systems, vendor-managed appliances. Leaving them open is not an option, and pretending they are fixed is worse. Mitigation engineering reduces the risk and documents what remains.

Technique	When it fits
Network isolation and segmentation	The vulnerable service only needs to reach a few systems
Virtual patching (IPS or WAF signatures)	A known exploit pattern can be blocked in front of the system
Application allow-listing	The system runs a small, stable set of software
Privilege reduction	Exploitation depends on rights the system's users do not need
Disabling the vulnerable feature or service	The function is not used in this environment

Each mitigated finding gets a residual-risk memo written for the AO: the vulnerability, why it cannot be patched, the compensating control, the evidence that the control works, and the remaining risk. BOD 26-02 adds a hard edge to this work for edge devices. Mitigation buys time, but the directive's 12- and 18-month deadlines require replacing end-of-support devices.

Proof of Closure

A finding is closed when an assessor will accept that it is closed. Three rules make that happen without rework.

- **Same tool, same policy.** Validation uses the same scanner and scan policy as the baseline. Switching tools at the end produces findings that do not match and disputes about what was fixed.

- **Evidence per finding.** Each closure package holds the before-and-after scan results, configuration diffs, the change record and screenshots where useful, stored in the agency's system of record (eMASS, CSAM, ServiceNow or Jira).
- **POA&M input.** Closures come with recommended POA&M updates and evidence references in the agency's format, so the ISSO can close items without rebuilding the proof.

The evidence format is agreed and sampled early. Changing it after the sample is approved is a change order, because reworking hundreds of evidence packages is where engagements lose weeks.

Two Delivery Modes

Mode A: Remediation Sprint

Phase	Typical timing	What happens
1. Kickoff and access	Weeks 1–2	Accounts and privileged access, change board introduction, data intake, baseline scan date frozen in writing
2. Normalization and prioritization	Weeks 2–3	Deduplication, asset and owner mapping, BOD 26-04 clock assignment, wave plan approved
3. Wave-based remediation	Weeks 3–12	Each wave runs test ring, change approval, deployment window and validation rescan, with an emergency lane for new top-tier items
4. Validation and evidence	Rolling; heaviest at the end	Closure evidence packages and POA&M input rows
5. Closeout and transition	Final 1–2 weeks	Metrics report, residual-risk memo, runbook handoff, optional move to managed mode

A single system boundary typically takes 8 to 10 weeks; a multi-system backlog takes up to 16. Each added enclave adds two to three weeks, and a backlog above about 5,000 raw findings usually means phased sprints or managed mode.

Mode B: Managed Patch Operation

A 12-month base with option years. Each month runs advisory intake (Patch Tuesday, vendor out-of-band releases and new KEV entries), the test ring, the change board, deployment windows, a validation scan and a metrics report. The emergency lane covers top-tier BOD 26-04 items during defined hours, and quarterly reviews refresh the residual-risk memo and the procedure.

The Avalon Team

Role	Sprint	Managed
Remediation lead / senior security engineer	0.75–1.0 FTE	0.25–0.5 FTE
Platform engineers (Windows, Linux, cloud, network as scoped)	1–3 FTE across waves	0.5–1.5 FTE equivalent
Compliance and evidence specialist	0.25 FTE	0.1–0.25 FTE
Project manager	0.1–0.25 FTE	0.1 FTE

What the Agency Provides

- Privileged access under agency control (agency-issued accounts or supervised sessions) by an agreed date. Access delays are the most common schedule killer.
- A standing slot at the change advisory board and committed maintenance windows. No windows, no throughput.
- Scan exports on a defined cadence, or read access to the scanner, using the same policy for baseline and validation.
- A test group or pre-production environment per major platform.
- System-owner approvals within agreed turnaround times, and a contact with authority to approve emergency-lane changes.
- The current asset inventory. Gaps found mid-engagement change scope through the change process.

What the Service Supports, and What It Does Not

Framework	What the service addresses
CISA BOD 26-04	The operational burden: triage against the four inputs, tiered remediation, forensic-triage coordination, and procedure updates
CISA BOD 26-02	Mitigation and replacement planning for end-of-support edge devices
NIST SP 800-53 Rev. 5	Implementation evidence for SI-2 flaw remediation, RA-5 (validation), CM-6 configuration settings and SI-5 advisories, interfacing with CM-3 change control and CM-8 inventory
NIST SP 800-37 Rev. 2	Closes Security Assessment Report findings and sustains the Monitor step
FISMA and IG metrics	Moves the vulnerability-management metrics IGs grade
FedRAMP	Remediation operations aligned to the new vulnerability rules, where agencies or providers need them
DISA STIGs and CORA (DoD)	Configuration remediation that maps to STIG closure and CORA indicators
NIST SP 800-171 and CMMC	For contractor environments: 3.14.1 flaw remediation and 3.11.2 and 3.11.3 scanning and remediation. CMMC Phase 2 certification was suspended July 13, 2026; the 800-171 obligations remain.

The accurate claims are specific: the service closes identified findings within directive timelines for the tiers in scope, produces assessor-ready closure evidence, reduces the open POA&M population, and documents residual risk for the AO. It does not achieve compliance, deliver an ATO, certify CMMC readiness, or guarantee an inspection result. Some findings are always unpatchable, authorization is an official's decision, and inspections grade programs, not sprints.

What the Service Does Not Include

Excluded	Where it belongs
Finding vulnerabilities in the first place	Vulnerability assessment and network testing. Validation rescans are the only scanning here.
Owning the POA&M lifecycle	A POA&M service. This engagement supplies closure input.
Full incident response	An incident response engagement, when triage confirms compromise
Deploying a new patching or scanning platform	A separate implementation
Fixing custom application code	DevSecOps or application modernization
Specialty, OT or medical device fleets	Separate terms or explicit exclusion

An Illustrative Sprint

The figures below are a planning illustration for one system boundary, not a quote and not a result from any engagement. The agency starts with 1,200 raw rows across its scanner exports, a penetration test report and open POA&M items. After deduplication (60% of rows are the same flaw on the same asset reported more than once) the backlog is 480 findings. Waves start in week 4, and the sprint is planned at 14 weeks for a fixed price of \$75K.

BOD 26-04 clock tier	Share (assumed)	Findings	Cleared by week
3 days (with forensic triage)	2%	10	2
14 days	18%	86	5
60 days	30%	144	8
Next system upgrade	50%	240	12

The top tier goes through the emergency lane during intake. The rest are worked in priority order at about 60 closures a week, with 10% of findings needing mitigation engineering, which is assumed to take twice the effort of a patch. The backlog clears in week 12, evidence packaging finishes in week 13, and 47 findings leave the sprint as documented compensating controls with residual-risk memos. The fixed price works out to about \$156 per finding closed.

When the Assumptions Change

Scenario	14-day tier cleared	60-day tier cleared	Backlog cleared	Sprint finish	Mitigated findings
Base case	Week 5	Week 8	Week 12	Week 13	47
Slow change board (35 closures a week)	Week 6	Week 11	Week 18	Week 19 (over plan)	47
More unpatchable systems (25%)	Week 5	Week 8	Week 13	Week 14	118

- **The change board sets the pace.** At 35 closures a week, which is what scarce maintenance windows typically allow, the same backlog takes 19 weeks. Committed windows are worth more than extra engineers.
- **Unpatchable systems add work, not failure.** With 25% of findings needing mitigation, the sprint still finishes within plan, but 118 findings leave as documented residual risk for the AO.
- **A legacy backlog is probably already past due.** BOD 26-04 clocks run from when a vulnerability is identified or listed, not from when a sprint starts. The sprint's job is to clear the highest-risk tiers first and document the rest honestly.

Appendix C lists every input. The agency's own scan data, tier mix and change-board cadence replace them in the normalization phase.

Pricing and Contracting

Scope	Typical shape	Market-norm range
Entry sprint	One system boundary, up to about 500 deduplicated findings, standard Windows and Linux; 6–10 weeks	\$45K–\$95K
Standard sprint	Multi-system, about 500–5,000 findings, mixed platforms; 10–16 weeks	\$100K–\$275K
Enterprise sprint	Multi-enclave, more than 5,000 findings, legacy-heavy; 16+ weeks or phased	\$275K–\$750K+
Managed operation, light	Up to about 500 endpoints and servers, one platform family	\$12K–\$25K a month
Managed operation, standard	Multi-platform, emergency lane, BOD 26-04 reporting	\$25K–\$60K a month

These are market-norm planning ranges, validated against the specific scope before any figure appears in a proposal.

Sprints are firm fixed price against a frozen baseline: a named scan export and date. New findings during the sprint go to the pre-priced emergency lane if they are top-tier, or to a change order. Managed operations are a fixed monthly price against a defined asset population, with a re-price trigger if the population moves outside an agreed band. Where a backlog is genuinely unknowable, a short time-and-materials discovery task converts into a fixed-price sprint. Per-finding performance pricing is not offered, because it is easy to game and hard to measure fairly.

Entry sprints fit under the simplified acquisition threshold of \$350,000 and can be bought as open-market purchases with one-year O&M funds, which makes them a natural year-end obligation for an agency with an embarrassing backlog.

Risks and How the SOW Contains Them

Risk	Containment
The moving baseline: new scans add findings mid-sprint	Baseline frozen to a named scan export and date; new items to the emergency lane or a change order
"While you're in there" work	An explicit exclusions list and a weekly parking-lot log that turns good ideas into priced follow-on work
Enclave creep	Enclaves named in the SOW; each addition priced
Evidence-format churn	Format agreed and sampled early; later changes by change order
No windows, late access, slow approvals	Agency obligations with due dates, an agency-attributable delay log from day one, and schedule relief tied to those dates
Validation with a different scanner	Same tool and policy for baseline and validation, in writing
Overstated outcomes	Approved language only: measured backlog reduction, clock compliance for defined tiers, evidence quality

Conclusion and Next Step

BOD 26-04 did not create the federal remediation backlog. It put a clock on it. Agencies that can only find flaws now need the capacity to fix them in tested waves, engineer around what cannot be fixed, and prove each closure in a form an assessor accepts.

The natural first step is an entry sprint: one system boundary, a frozen baseline, a fixed price and a defined exit. Avalon takes one bounded engagement at a time, in unclassified environments on standard Windows, Linux and cloud platforms, using the agency's own tools. The emergency lane is offered for defined hours rather than as a round-the-clock commitment. Avalon is a small business without prior federal contracts under this service and says so; the fixed-price, single-boundary structure is built to keep the agency's exposure small. To discuss a sprint, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

BOD: Binding Operational Directive

A CISA directive that federal civilian agencies must follow. BOD 26-04 sets risk-based remediation clocks; BOD 26-02 addresses end-of-support edge devices.

CAB: Change Advisory Board

The body that approves changes to production systems.

CORA: Cyber Operational Readiness Assessment

DoD's inspection regime for cyber readiness, which replaced the earlier command cyber readiness inspections.

EPSS: Exploit Prediction Scoring System

A model estimating the probability that a vulnerability will be exploited.

KEV: Known Exploited Vulnerabilities

CISA's catalog of vulnerabilities with evidence of active exploitation.

Mitigation engineering

Designing compensating controls for a vulnerability that cannot be patched, and documenting the residual risk.

SSVC: Stakeholder-Specific Vulnerability Categorization

A decision-tree method for prioritizing vulnerabilities by exploitation, exposure and impact.

STIG

A DISA Security Technical Implementation Guide: a configuration baseline for DoD systems.

Test ring

A designated group of systems where updates are applied and observed before wider deployment.

Virtual patching

Blocking exploitation of a vulnerability with a network or application filter instead of changing the vulnerable software.

Appendix B: Control Map

Control	Name	Evidence the engagement produces
SI-2	Flaw remediation	Wave records, closure evidence packages, metrics
RA-5	Vulnerability monitoring and scanning	Validation rescans with the baseline scanner and policy
CM-6	Configuration settings	STIG and CIS remediation with SCAP results
SI-5	Security alerts, advisories and directives	Advisory intake and BOD 26-04 clock assignments
CM-3	Configuration change control	Change board packages and approvals per wave
CM-8	System component inventory	Asset and owner mapping from normalization
CA-5	Plan of action and milestones	POA&M closure input and residual-risk memos
800-171 3.14.1, 3.11.2, 3.11.3	Flaw remediation; vulnerability scanning and remediation	The same evidence, for contractor environments

Appendix C: Illustration Assumptions

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

Assumption	Value	Basis
Raw findings	1,200 rows	Scanner exports, a penetration test report and open POA&M items

Assumption	Value	Basis
Duplicate share	60%	The same flaw on the same asset reported by more than one source
Clock tier mix	3 days (with forensic triage) 2%, 14 days 18%, 60 days 30%, Next system upgrade 50%	Planning assumption
Closure rate	60 a week (base); 35 a week (slow change board)	Planning assumption
Share needing mitigation	10% (base); 25% (alternate)	Planning assumption; mitigation takes twice the effort
Waves start	Week 4	After kickoff, access and normalization
Planned sprint length	14 weeks	Within the 8–16 week range
Price	\$75K	Inside the \$45K–\$95K entry-sprint band
Excluded	Incident response, new tooling, application code fixes	Outside the engagement

Appendix D: References

1. **Cybersecurity and Infrastructure Security Agency**, *BOD 26-04: Prioritizing Security Updates Based on Risk*, June 10, 2026
<https://www.cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk>
2. **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>

3. **BleepingComputer**, *CISA Orders Federal Agencies to Replace End-of-Life Edge Devices (BOD 26-02)*, February 2026
<https://bleepingcomputer.com/news/security/cisa-orders-federal-agencies-to-replace-end-of-life-edge-devices>
4. **Crowell & Moring**, *Time for a Change: FedRAMP Fundamentally Revamps Program With Consolidated Rules for 2026*, July 7, 2026
<https://www.crowell.com/en/insights/client-alerts/time-for-a-change-fedramp-fundamentally-revamps-program-with-consolidated-rules-for-2026>
5. **National Institute of Standards and Technology**, *SP 800-40 Rev. 4, Guide to Enterprise Patch Management Planning*, April 2022
<https://csrc.nist.gov/pubs/sp/800/40/r4/final>
6. **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>
7. **Defense Information Systems Agency**, *Security Technical Implementation Guides*
<https://public.cyber.mil/stigs/>
8. **FIRST**, *Exploit Prediction Scoring System (EPSS)*
<https://www.first.org/epss/>
9. **McGuireWoods**, *DoW Suspends CMMC Phase II Requirements, Launches 60-Day Review*, July 14, 2026
<https://blogs.mcguirewoods.com/2026/07/14/dow-suspends-cmmc-phase-ii-requirements-launches-60-day-review/>
10. **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/>