

REMEDiation & PATCH MANAGEMENT

Avalon clears your backlog of open vulnerabilities and audit findings in prioritized waves, testing patches first, then handing back documented proof each fix worked.

THE PROBLEM WE ADDRESS

CISA's BOD 26-04 gives civilian agencies as little as three calendar days to fix the most dangerous flaws, and requires checking whether attackers already got in, a tempo most O&M staffing was never built for.

Two decades of federal investment in scanning built world-class vulnerability visibility without funding the labor to close findings, few agencies can staff the closure rate they require.

WHAT WE DO

- Findings intake and normalization across scanners, pen tests, and IG/GAO findings
- Risk-based prioritization aligned to BOD 26-04's exposure/KEV/impact model
- EPSS exploit-prediction scoring and agency mission-context weighting
- Patch acquisition, validation, and staged test-ring deployment
- Deployment through the agency's existing tooling (MECM/Intune, Tanium, BigFix, Ansible)
- Configuration remediation against DISA STIG and CIS Benchmark deviations
- Compensating controls, documented, for what can't be patched
- Rescan validation with before/after diffs, packaged as assessor-ready evidence

HOW WE DO IT

1 KICKOFF & ACCESS

Privileged-access mechanics, CAB introduction, and a baseline snapshot frozen in writing.

DELIVERABLE

Frozen baseline snapshot

3 WAVE-BASED REMEDIATION

Each wave runs test ring, CAB approval, deployment, and validation rescan, with an emergency lane for new critical items.

DELIVERABLE

Closed findings, wave by wave

2 BACKLOG NORMALIZATION

Dedupe, asset/owner mapping, BOD 26-04 clock assignment, and an approved wave schedule.

DELIVERABLE

Prioritized wave schedule

4 EVIDENCE & CLOSEOUT

Closure evidence packages, a metrics report, and a residual-risk memo, with an option to convert to managed operations.

HANDOVER

Closure evidence package

VALUE DELIVERED

- › **Fixes tested before they ship.** Every wave runs through a test ring with a written rollback plan — no patch breaks mission systems.
- › **Evidence an assessor accepts.** Before/after rescan diffs are packaged into assessor-ready closure evidence, not just a checked box.
- › **The right clock on every finding.** BOD 26-04's four-variable model assigns the correct remediation timeline instead of treating every finding the same.
- › **Coverage for the unpatchable.** Compensating controls and residual-risk memos give the AO a documented path forward.

COMMONLY PROCURED AS

Vulnerability remediation / patch management services

AT A GLANCE

Model	Fixed-price or T&M, scoped per engagement
Typical	8–16 wks per sprint (option to convert to managed ops)
NAICS	541512, 541511, 541519, 541611, 541690
UEI	Y9MXMMHY3HA1
CAGE	242T0
Standards	CISA BOD 26-04, NIST SP 800-40 Rev. 4, NIST SP 800-53 SI-2/RA-5/CM-6

WHO WE WORK WITH

- ISSO / system owner sitting on a growing scanning backlog
- CISO staff facing a BOD 26-04 remediation clock
- AO needing residual-risk documentation for the unpatchable

COMMITMENT TO QUALITY

Avalon is led directly by a PMP-certified founder with a decade of enterprise engineering experience where every engagement gets senior-level attention, never a subcontracted bench. Delivery follows NIST SP 800-53, RMF, and FISMA, evidence-backed and control-mapped by design. ISO 9001/27001 is on the roadmap as the pipeline scales.

Status: Small business federal contractor based in Los Angeles, CA

CISA BOD 26-04

NIST SP 800-40 REV. 4

NIST SP 800-53 SI-2/RA-5/CM-6

Under a three-day clock, mobilization speed is the product.

Brandon Ireland, CEO

| (714) 655-3863

| partner@avalontechservices.com

| avalontechservices.com