



Securing Tomorrow's Missions Today.



Past the Perimeter: What an Attacker Reaches After the First Foothold

External & Internal Network Testing: a fixed-price, rules-of-engagement penetration test of one unclassified boundary that shows how far an intruder gets and whether your monitoring sees it.

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
Why Scans and Assessments Leave the Question Open	3
Why the Inside Matters Most	3
The Mandates and the Calendar	4
What the Engagement Does	6
What Sets the Internal Phase Apart	7
Deliverables	8
How It Relates to Vulnerability Assessment	8
Evidence Assessors Can Use	9
How an Engagement Runs	10
What the Agency Provides	10
What Is Not Included	11
How Avalon Staffs It	12
Pricing and How to Buy	13
Illustration: Hours, Calendar and Price for One Boundary	13
Price Across the Rate Band	14
Retest and Schedule Sensitivity	15
Common Pitfalls	16
Conclusion and Next Step	16
Appendices	17
Appendix A: Glossary	17
Appendix B: Illustration Assumptions	17
Appendix C: References	18

Executive Summary

Most federal systems are assessed on paper far more often than they are attacked under controlled conditions. Security control assessments confirm that controls are documented and switched on. Vulnerability scans list what might be wrong. Neither answers the question an Authorizing Official, an inspector general or a new CISO eventually asks: if someone got in, how far could they go, and would we notice?

A network penetration test answers that question directly. Testers work first from the internet against the agency's exposed services, then from inside the network as if an attacker already holds a foothold: a phished workstation, a rogue device or a compromised contractor account. The internal half is where the worst breaches play out, because many federal networks are still flat and over-trusted on the inside. NIST SP 800-53 Rev. 5 names this work as its own control, CA-8 (Penetration Testing).

This paper is for the people who need that answer and pay for it: CISOs who fund testing, ISSMs and ISSOs who request it and carry its findings into the authorization package, system owners and Authorizing Officials who decide on risk, and the CORs who buy the work. It describes Avalon Technology Services' External & Internal Network Testing service, which starts with one engagement:

- **A fixed-price combined test of one unclassified system boundary.** External testing of one internet-facing footprint, then internal testing from an assumed foothold in one segment with one Active Directory domain, under a signed rules of engagement (ROE). Two to four weeks of active testing inside a six to ten week window from ROE to final report.
- **Two things a scan cannot give.** Attack paths from the foothold to domain control and to named data stores, ranked by what actually cuts them, and a detection observation record of whether the agency's monitoring saw each step.

Section 9 works through an illustrative engagement: 246 hours across a lead tester, a project manager, a compliance mapper and a QA reviewer, about seven calendar weeks, and a fixed price of \$49.2K at a \$200 an hour planning rate. That sits inside the \$40,000 to \$120,000 range typical for a combined federal test of this size, and well under the \$350,000 simplified acquisition threshold.

A penetration test is a point-in-time, scope-bounded assessment. It produces control-mapped evidence that supports the RMF Assess step and the annual FISMA assessment. It does not grant an authorization or guarantee a clean result; the agency's assessor draws conclusions and the Authorizing Official decides.

Why Scans and Assessments Leave the Question Open

Agencies already spend heavily on knowing what is wrong. What they rarely have is evidence of what an attacker could do with it. The gap shows up in the same phrases across programs.

What the ISSM or CISO hears	What it usually means
"Our ATO expires in nine months and the assessor wants a pen test."	CA-8 is selected or tailored in, and there is no current exploitation-based evidence
"We scan constantly, but we don't know what an attacker could actually do."	Thousands of scanner findings, none validated, none chained into a path
"The IG dinged us on CA-8."	A finding that needs a dated, scoped test with a signed ROE behind it
"We're flat inside and moving to Zero Trust."	No baseline of how far one compromised host reaches today
"If someone got domain admin, would the SOC even see it?"	Detection has never been exercised against real attacker behavior

Why the Inside Matters Most

- **Flat networks.** Decades of "hard shell, soft center" design mean one compromised workstation can often reach servers, management interfaces and directory services it has no business touching.
- **Identity is the real perimeter.** Active Directory trust relationships, stale service accounts and over-privileged groups usually decide how fast an intruder moves, and no external scan sees them.
- **Edge devices are the usual front door.** End-of-support firewalls, routers and VPN appliances are a recurring entry point, which is why CISA BOD 26-02 sets deadlines to inventory and retire them. They are the external phase's first targets.
- **Monitoring is rarely tested.** Logging investments are measured by what is collected, not by whether a real attack sequence raises an alert someone acts on.

The Mandates and the Calendar

Driver	What it requires	What it means for a network test
NIST SP 800-53 Rev. 5, CA-8	Penetration testing at an organization-defined frequency; in the High baseline, tailorable into Moderate	The direct control. CA-8(1) calls for an independent tester; CA-8(2) red teaming is scoped separately
CA-2, CA-7, RA-3, RA-5, SI-2	Control assessment, continuous monitoring, risk assessment, vulnerability scanning, flaw remediation	The test validates scan output, feeds the risk assessment and hands findings to remediation
NIST SP 800-37 Rev. 2 and SP 800-53A Rev. 5	RMF Assess step; assessment procedures	Test results become dated evidence in the assessment record; the AO decides in Authorize
NIST SP 800-115	Technical guide to security testing and assessment	The federal methodology baseline, with PTES and MITRE ATT&CK for structure and reporting
CISA BOD 26-04 (Jun 10, 2026)	Risk-based remediation clocks; replaced BOD 22-01 and BOD 19-02	Exploited findings land on the same clocks; Avalon's Vulnerability Assessment & Exploitation paper covers the triage
CISA BOD 26-02 (Feb 6, 2026)	End-of-support edge devices: inventory in 3 months, decommission in 12, replace in 18	Edge devices still in service are tested first
OMB M-26-14 (May 2026)	A risk-based logging model; replaced M-21-31	Detection observation is written against the agency's own M-26-14 priorities

Driver	What it requires	What it means for a network test
DoD CSRMC (Sep 24, 2025)	Cybersecurity risk management construct announced; RMF, DoDI 8510.01 and eMASS remain in use	For unclassified DoD systems, results go into the existing RMF record

Two common assumptions need correcting. NIST SP 800-171, and so CMMC, has no explicit penetration testing requirement; it calls for periodic security assessment (3.12.1) and vulnerability scanning (3.11.2). CMMC Phase 2 was suspended on July 13, 2026, while Phase 1 self-assessment and 800-171 obligations remain. And the annual FedRAMP penetration test applies to cloud service providers, must be performed by a FedRAMP Recognized assessor, and covers the provider's offering only. The agency still authorizes its own systems, and those systems still need their own CA-8 evidence.

Tests get bought at predictable moments: an initial authorization, a three-year reauthorization or a significant change; the annual FISMA cycle; an inspector general or GAO finding on CA-8; an incident or near miss; a new system, cloud migration or network re-architecture; a Zero Trust program that needs a segmentation baseline; and fiscal year-end operations and maintenance funds, which peak in August and September.

What the Engagement Does

The test is human-driven and time-boxed. Scanners are an input, not the product. Every finding in the report has been validated by a tester, and every exploitation step was authorized in advance by the ROE.

Workstream	Activities
Reconnaissance and enumeration	Map the real attack surface: live external addresses, hostnames and exposed services; on the inside, segments, hosts, directory services and trust relationships in scope
Authenticated and unauthenticated discovery	Open-source intelligence and unauthenticated scanning from outside; scoped authenticated enumeration from the foothold
Vulnerability validation	Confirm which scanner findings are real and reachable, and discard false positives
Controlled exploitation	Prove exploitability under the ROE without disrupting production, then stop
Post-exploitation and lateral movement (internal)	Privilege escalation, Active Directory and trust-path abuse, segmentation checks, and proof of reach to named data stores
Detection and response observation	Record, step by step, whether the agency's monitoring logged, alerted and escalated
Analysis, risk rating and reporting	Findings rated by exploitability and mission impact, mapped to 800-53 controls and ATT&CK techniques

What Sets the Internal Phase Apart

A scan ranks findings one at a time, by severity score. An intruder does not. An intruder chains a weak service account, an over-broad access rule and a missing segmentation boundary into a path to domain control. The internal phase reports those paths and names the few choke points (often one access rule, one service account or one firewall rule) whose removal cuts most of them. Fixing a choke point can matter more than fixing ten high-severity findings that sit on no path at all.

Detection observation is the second distinctive output. For each step the testers take, the report records whether it appeared in the agency's logs, whether an alert fired and whether anyone escalated. Gaps map to AU-6 and SI-4 and to the agency's M-26-14

logging priorities. This requires the SOC to share its log and alert exports for the test window, and it is agreed in the ROE whether the SOC is told about the test in advance.

Deliverables

Deliverable	Format
Rules of engagement and test plan: scope, targets, windows, methods, hands-off systems, emergency contacts	Signed PDF
Executive summary report	PDF, leadership-ready
Technical findings report: evidence, severity, affected assets, attack paths, remediation guidance	PDF plus optional CSV or JSON export
Control-mapping appendix: CA-8, RA-5 and other implicated 800-53 controls	Table, ready for the assessment record and POA&M
Remediation-priority matrix: exploitability by mission impact	Table
Out-brief with slides	Live briefing
Retest attestation, if bundled	PDF addendum

How It Relates to Vulnerability Assessment

Avalon's Vulnerability Assessment & Exploitation service is a separate offer with its own paper. It owns validated scanning, proof-then-stop exploitation of individual findings and BOD 26-04 triage, and it prices single-phase network tests and a system-level test that adds one web application. This service owns the combined engagement: the internal attack chain from a foothold, segmentation validation, reach to named data stores and detection observation. The two are priced from the same rate card, so the same tester hours are never sold two ways.

Evidence Assessors Can Use

Control	Evidence the test produces
CA-8	Signed ROE, dated test record, validated findings and attack paths
CA-8(1)	Testing by a party independent of the team that built or operates the system
RA-5	Scanner findings validated or discarded, with reasons
RA-3	Exploitability and mission-impact ratings to feed the risk assessment
CA-2 and CA-7	Dated input to the assessment and the continuous monitoring record
SI-2	Remediation-priority matrix for flaw remediation and the POA&M
AU-6 and SI-4	Detection observation: what was logged, alerted and escalated

The accepted way to describe it: this engagement provides exploitation-based testing that directly addresses NIST SP 800-53 CA-8 and produces control-mapped evidence to support the RMF Assess step and the annual FISMA assessment.

Accurate	Not accurate
Exploitation-based evidence for CA-8	Achieves or speeds your ATO
A point-in-time, scope-bounded assessment	Proves the network is secure
Control-mapped findings for the assessment record	Makes you FedRAMP Certified or CMMC compliant
A record of what monitoring did and did not see	Certifies the SOC effective

How an Engagement Runs

Phase	Typical duration	Base case	What happens
Scoping and rules of engagement	1–2 weeks (agency-gated)	Wk 1–2	Targets, ranges, windows, hands-off list, emergency stop; ROE and authorization-to-test letter signed
Kickoff and access setup	2–4 days	Wk 3	Network drop, VPN or jump box; scoped credentials; contacts and de-confliction
External testing	3–7 days	Wk 3–4	Recon, enumeration, validation and controlled exploitation of internet-facing assets
Internal testing	5–10 days	Wk 4–6	Foothold enumeration, privilege escalation, lateral movement, proof of reach to data
Analysis and reporting	5–7 days	Wk 6–7	Risk rating, attack paths, control mapping, detection observation, draft report
Out-brief and delivery	2–3 days	Wk 7	Executive and technical read-outs; final report
Retest (optional)	2–5 days	After fixes	Re-verify remediated findings; retest attestation

Nothing starts before the ROE is signed, including reconnaissance. Active testing in the base case is 13 business days, and the full window is about 7 weeks. Scoping and access are the long pole, and the agency controls both, so the statement of work ties delivery dates to timely access with day-for-day relief when it arrives late.

What the Agency Provides

- A point of contact with authority to make scope and de-confliction decisions in real time.

- A signed ROE, an authorization-to-test letter, and confirmation that the agency owns or controls every in-scope asset.
- Access for the internal phase: an on-site network drop, VPN or jump box, and any credentials scoped for authenticated testing.
- A defined testing window and an emergency-stop and escalation procedure.
- Log and alert exports for the test window, so detection observation can be completed.
- Network diagrams, an asset inventory, recent scan results and the SSP boundary where available. These are optional, but they lower cost and sharpen scope.

What Is Not Included

Included	Separate work
Validated, exploitation-based testing	Recurring vulnerability scanning on its own
Prioritized remediation guidance and an optional retest	Performing the fixes
Network services an attacker reaches, including exposed web services	Deep web application or API testing
Time-boxed, broad-coverage testing	Red teaming (CA-8(2)), scoped separately
Technical testing under the ROE	Phishing, social engineering or physical testing, unless named in the SOW and ROE
Agency systems the agency authorizes	The annual FedRAMP test of a cloud provider
Safe, controlled exploitation	Denial-of-service or destructive testing
One point-in-time engagement	Continuous monitoring
Unclassified systems	Classified systems or cleared on-site work

How Avalon Staffs It

Avalon takes one engagement at a time, works business hours unless a named partner covers an agreed off-hours testing window, and works in unclassified environments only. Testing happens only under the agency's written authorization and a signed ROE, and Avalon never tests a system it built or operates. Avalon has no past federal engagements under this service. Each engagement is delivered by named people listed in the proposal, so the agency evaluates the testers, the methodology and the ROE controls rather than a brand.

Requirement	How it is handled
Lead tester	Named personnel whose certifications (OSCP-class or equivalent) and investigation level match the agency's requirements, listed in the proposal, hired or subcontracted
QA reviewer	A second credentialed tester, subcontracted, who reviews findings and ratings before delivery
Compliance mapper	Subcontracted; maps findings to 800-53 controls and the agency's POA&M format
Project manager	Avalon's founder: ROE administration, de-confliction, status reporting and deliverable QA
Tooling	Licensed commercial scanning and exploitation tools in place before the ROE is signed, as a condition of the engagement
DoD privileged access	Personnel qualified under DoD 8140 for the relevant work role, as a condition of the engagement
Insurance and contract vehicles	Coverage the solicitation requires is bound before the ROE is signed; Avalon does not hold a GSA Schedule or a governmentwide contract today

Pricing and How to Buy

Engagement	Range	Where it is offered
Combined external and internal test, one boundary, with attack paths and detection observation	\$40K–\$120K	This service, firm fixed price
External network test only	\$10K–\$30K	Vulnerability Assessment & Exploitation
Internal network test only	\$12K–\$40K	Vulnerability Assessment & Exploitation
System-level test that adds one web application	About \$65K	Vulnerability Assessment & Exploitation
Retest after agency fixes	8%–18% of base	Named optional line, either service

Every price is a firm fixed price with an itemized basis: hours by role times rate, plus a clearly named optional retest line. Initial pricing is anchored at the lower to middle of the range. Contingency or outcome pricing is declined, because a test that finds more should not cost more, and a test that finds less should not cost less.

All of these engagements fit under the \$350,000 simplified acquisition threshold and can be bought open-market. 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. Testing inside a larger assessment or security task order can be subcontracted to Avalon by the prime. Avalon does not hold a GSA Schedule or a governmentwide contract today.

Adding the test to the incumbent operations contract has one structural weakness: CA-8 expects objectivity, and the team that runs the network would be testing its own work.

Illustration: Hours, Calendar and Price for One Boundary

The figures below are a planning illustration for one representative unclassified Moderate system, not a quote and not a result from any engagement. Every day count and hour is an assumption drawn from typical phase durations.

The assumed scope is one system boundary with one external footprint and one internal segment holding one Active Directory domain. A named lead tester carries the technical work, Avalon's founder manages the engagement, and a subcontracted compliance mapper and QA reviewer support the reporting gate.

Role	Basis	Hours
Lead tester	External 5 days, internal 8, reporting 6, setup and out-brief 3; 8 hours a day	176
Project manager	About 10% across a seven-week window	40
Compliance mapper	Concentrated in reporting	24
QA reviewer	Report gate review	6
Total		246

Price Across the Rate Band

Scenario	Hours	\$150/hr	\$200/hr	\$250/hr
Base: one boundary, one internal segment	246	\$36.9K	\$49.2K	\$61.5K
S1: second internal segment, half-time supporting tester	392	\$58.8K	\$78.4K	\$98.0K
KB low-end days	164	\$24.6K	\$32.8K	\$41.0K
KB high-end days	328	\$49.2K	\$65.6K	\$82.0K

At the \$200 planning rate the base case is \$49.2K, in the lower to middle of the \$40K to \$120K range. At \$250 it is \$61.5K. At \$150 it computes to \$36.9K, below the range floor, so the floor governs. A second internal segment with a half-time supporting tester (S1) adds internal and reporting days and comes to 392 hours, \$58.8K to \$98.0K. The low and high ends of the typical phase durations bracket the base: 164 hours (\$24.6K at \$150) and 328 hours (\$82.0K at \$250).

The base case also sits inside the combined external and internal bands of the Vulnerability Assessment & Exploitation paper (\$22.0K to \$70.0K) and below its system-level tier, which adds a web application. Every scenario is far under the simplified acquisition threshold.

Retest and Schedule Sensitivity

Change	Added hours	Added at \$200/hr	Share of base
Bundled retest, 2 lead days plus 4 PM hours	20	\$4.0K	8%
Bundled retest, 3 lead days plus 4 PM hours	28	\$5.6K	11%
Bundled retest, 5 lead days plus 4 PM hours	44	\$8.8K	18%
ROE or access slips 4 calendar weeks (PM at about 10%)	16	\$3.2K	7%

A retest is priced as a named line, so the agency can buy it with the base or later. An agency-side slip is handled by change order rather than absorbed, which keeps the fixed price honest for both sides.

Common Pitfalls

Pitfall	How to avoid it
"While you're in there" scope creep	A fixed target list in the ROE; additions by change order
A scan sold as a penetration test	Ask for validated findings, attack paths and the tester's named credentials
Testing before the paperwork	No activity, including reconnaissance, before the ROE and authorization letter are signed
Access delays eating the schedule	Access confirmed at kickoff; day-for-day relief written into the SOW
Overselling the compliance value	Use the accurate phrasing; the assessor concludes and the AO decides
Inconsistent pricing across testing line items	One rate card; single-phase tests and the system-level test priced in one place
Reports nobody can file	Control-mapped findings in the agency's POA&M format

Conclusion and Next Step

A scan tells an agency what might be wrong. A control assessment tells it what is written down. A combined external and internal penetration test tells it how far an intruder actually gets, which handful of fixes cut the most attack paths, and whether the SOC saw any of it. That is dated, control-mapped evidence an ISSM can file, an assessor can use and an Authorizing Official can weigh.

The natural first step is a fixed-price combined test of one unclassified boundary, under a signed ROE and well under the simplified acquisition threshold. Where budget is tighter, an external-only test through the Vulnerability Assessment & Exploitation service is a smaller start. To discuss a test, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

Attack path

A chain of weaknesses an attacker can use in sequence to move from a foothold to a target, such as domain control or a named data store.

Choke point

A single access rule, account or segmentation boundary whose removal cuts many attack paths at once.

Detection observation

A step-by-step record of whether the agency's monitoring logged, alerted on and escalated the testers' activity.

Foothold

The assumed starting point for internal testing, such as one compromised workstation or account.

PTES

Penetration Testing Execution Standard, a community methodology used alongside NIST SP 800-115.

Rules of engagement (ROE)

The signed document that authorizes testing and sets scope, targets, windows, methods, hands-off systems and the emergency stop.

Appendix B: Illustration Assumptions

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

Assumption	Value	Basis
Scope	One boundary, one external footprint, one internal segment, one AD domain	Planning assumption
Phase durations	ROE 1–2 weeks; kickoff 2–4 days; external 3–7; internal 5–10; reporting 5–7; out-brief 2–3	Typical federal engagement
Lead tester days	22 in the base case, 8 hours a day	Planning assumption
Other roles	PM 40 hours; compliance 24; QA 6	Planning assumption
Rates	\$150–\$250 an hour fully burdened; fee at \$200	One Assessment & Testing rate card
Price check	Base \$49.2K	Inside the \$40K–\$120K combined range
Retest	2–5 lead days plus 4 PM hours	Typical retest duration

Appendix C: References

1. **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>
2. **National Institute of Standards and Technology**, *SP 800-53A Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations*
<https://csrc.nist.gov/pubs/sp/800/53/a/r5/final>
3. **National Institute of Standards and Technology**, *SP 800-115, Technical Guide to Information Security Testing and Assessment*
<https://csrc.nist.gov/pubs/sp/800/115/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. **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>
6. **Cybersecurity and Infrastructure Security Agency**, *Binding Operational Directives (BOD 26-02, BOD 26-04)*
<https://www.cisa.gov/news-events/directives>
7. **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>
8. **General Services Administration**, *FedRAMP*
<https://www.fedramp.gov>
9. **MITRE**, *ATT&CK*
<https://attack.mitre.org>
10. **PTES**, *Penetration Testing Execution Standard*
<http://www.pentest-standard.org>
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/>