



Securing Tomorrow's Missions Today.



Will Your App Survive the Next OS Release? A Fixed-Fee Security, Accessibility and Release- Readiness Assessment for One Agency Mobile App

Mobile Development: find out whether your agency's app can still ship, whether it passes vetting and Section 508 review, and whether to keep, rebuild or retire it

AvalonTechServices.com

contact@AvalonTechServices.com

Executive Summary	2
Why Agency Apps Stop Shipping	3
Why It Concentrates in Government	3
The Standards and the Calendar	4
What the Assessment Does	6
Security Verification	7
Accessibility Testing	7
Release Readiness	7
The Keep, Rebuild or Retire Memo	7
Deliverables	8
Where the Engagement Stops	8
Evidence the Reviewers Can Use	9
How an Engagement Runs	10
What the Agency Provides	10
What Is Not Included	11
How Avalon Staffs It	11
Pricing and How to Buy	13
Illustration: One App, Two Platforms	13
What the Engagement Costs	14
What Keeping the App Costs	15
Common Pitfalls	15
Conclusion and Next Step	16
Appendices	16
Appendix A: Glossary	16
Appendix B: Illustration Assumptions	17
Appendix C: References	17

Executive Summary

Many agency mobile apps were built once, by a vendor who has since moved on. Every year Apple and Google ship new operating system releases and raise the minimum SDK and target-API levels an app update must meet. An app nobody has touched in two or three years starts to crash on new phones, gets flagged in the store, or cannot be updated at all because nobody knows who holds the signing keys. At the same time it may be failing Section 508 for screen reader users, and it may never have been through the agency's mobile app vetting process.

Those are three problems with one root cause: nobody owns an honest picture of the app, so nobody can say whether to fix, rebuild or retire it.

This paper is for the people who own that decision: the mission program manager who funds the app, the CIO or digital services lead who sets the standards, the ISSO or ISSM who approves it, the Section 508 coordinator, and the COR who buys the work. It describes Avalon Technology Services' Mobile Development service, which starts with one engagement:

- **A fixed-fee security, accessibility and release-readiness assessment for one existing iOS or Android app.** About three to five weeks. OWASP MASVS-L1 verification with static and dynamic testing and a gap list against a NIST SP 800-163 Rev. 1 vetting evidence package; manual VoiceOver and TalkBack testing of named critical flows with a draft Accessibility Conformance Report (ACR) gap list; a release-readiness check of SDK currency, account ownership, signing and MDM compatibility; an authentication review; a keep, rebuild or retire memo; and a priced remediation backlog. It is priced inside the market band for a discovery sprint (\$35K to \$75K); Avalon quotes it firm fixed price at \$35K to \$65K.
- **A conditional build or sustainment follow-on.** The remediation backlog maps to a priced build or sustainment tier, bought separately if the agency chooses.

Section 9 works through an illustrative app on two platforms with 8 critical flows and 3 integrations. The assessment takes 282 hours, or \$33.8K to \$52.2K at the KB blended rate band, with an illustrative fee of \$43K.

Avalon builds to the standards, produces the evidence and supports the agency's reviewers. The agency's ISSO and Authorizing Official decide on security, the 508 office decides on conformance, and Apple and Google decide on store approval. Avalon does not issue or guarantee any of those outcomes.

Why Agency Apps Stop Shipping

The phrases below come up in almost every conversation about an aging agency app. Each points to an app with no current owner of its security, accessibility or release state.

What the program says	What it usually means
"Our app hasn't been updated since 2022 and crashes on new phones."	The app targets an old SDK and the build toolchain has not been updated since the last vendor left
"We got a 508 complaint about the app."	Components were never tested with VoiceOver or TalkBack, and no ACR exists
"The security office won't put it on managed devices."	No vetting evidence exists for the agency's SP 800-163 process
"We don't know who holds the developer account."	The app was published under a vendor's account, or signing keys left with the vendor
"The CIO shop says we have to justify why this can't just be the website."	No written decision on native versus responsive web was ever made

Why It Concentrates in Government

- **Apps are bought as projects, not products.** The build is funded once; sustainment is severable money that often never arrives, so the app ages until it breaks.
- **Federal authentication is not a password.** Public apps integrate Login.gov; workforce apps use agency ICAM or derived PIV credentials (NIST SP 800-157), and each adds review steps.
- **Every federal app carries a legal accessibility duty.** Section 508 applies to agency apps whether or not a consumer app shop built them to it.
- **Software assurance is risk-based.** OMB M-26-05 (January 23, 2026) rescinded M-22-18 and M-23-16. Each agency sets its own software assurance policy, so each program decides what evidence its app needs.

The Standards and the Calendar

Driver	What it says	What it means for this engagement
Section 508 (36 CFR Part 1194, 2017 refresh)	Incorporates WCAG 2.0 Level AA by reference for federal ICT, including apps	The formal baseline; the assessment also tests to WCAG 2.1 and 2.2 AA, the current W3C guidance
21st Century IDEA Act (2018)	Federal digital services must be accessible, consistent, mobile-friendly and user-centered	Grounds the native-versus-web question in the keep, rebuild or retire memo
NIST SP 800-163 Rev. 1	Vetting the security of mobile applications before agency use	The gap list shows what the vetting evidence package is missing
NIST SP 800-124 Rev. 2	Managing the security of mobile devices in the enterprise	Checks that deployment fits the agency's MDM posture and device policies
OWASP MASVS and MASTG	A mobile security verification standard and testing guide; L1 is the baseline	The verification method; a methodology, not a government approval
NIST SP 800-53 Rev. 5	SA-11 and SA-15 developer testing and process, plus SC, IA, AC, AU and CM controls	The control IDs in the evidence map for the ISSO
OMB M-26-05 (Jan 23, 2026)	Agencies set risk-based software assurance policies; NIST SP 800-218 (SSDF) is guidance	An SBOM is an optional contract term the agency may choose, not a mandate
FedRAMP Consolidated Rules (Jun 25, 2026)	Cloud offerings are "FedRAMP Certified" in classes A through D; certification covers the provider's offering only	Every third-party service the app calls (analytics, crash reporting, push beyond Apple and Google) must be certified or inside the agency boundary

Where an agency names NIAP protection profiles, the assessment notes them; Avalon does not perform NIAP evaluations. Where defense contractors handle Controlled Unclassified Information on mobile devices, NIST SP 800-171 requirements 3.1.18 and 3.1.19 apply to the contractor organization, not the app.

Common triggers: a new iOS or Android release breaks the app or the store flags an outdated SDK; the incumbent's contract ends; a 508 complaint, inspector general finding or congressional letter; a poor public rating; and fourth-quarter funds in July through September 2027, since a fixed-scope assessment is a defined, non-severable service.

What the Assessment Does

The assessment covers one existing app, on one or both platforms, workforce or public. It works in the agency's own repositories, developer accounts and test distribution, and installs nothing of Avalon's. Static and dynamic testing runs with MobSF, an open-source mobile security framework, inside an environment the agency approves.

Step	Activities
Kickoff and access	Repository, build and test-distribution access agreed; critical flows, device baseline and integrations named; government dependencies dated in writing
Security verification	MASVS-L1 verification with MobSF static and dynamic testing; findings mapped against an SP 800-163 Rev. 1 vetting evidence package
Accessibility testing	Manual VoiceOver and TalkBack testing of each named critical flow; criterion-level draft ACR gap list
Release readiness	SDK and target-API currency, build toolchain, signing key custody, Apple and Google account ownership, MDM compatibility
Authentication review	Login.gov, agency ICAM or derived PIV integration checked against the agency's identity policy
Decision and backlog	Keep, rebuild or retire memo; priced remediation backlog; readout to the program office, ISSO and 508 coordinator

Security Verification

MASVS-L1 is the baseline for most civilian apps. The verification covers on-device storage, cryptography, authentication, network communication, platform interaction and code quality, plus a check that no sensitive data travels through Apple or Google push services. The output is a finding list by MASVS control and a gap list that tells the ISSO which pieces of an SP 800-163 vetting package exist today and which do not. It is not a penetration test.

Accessibility Testing

Automated scanners miss most mobile accessibility problems. The 508 specialist tests each named critical flow by hand with VoiceOver on iOS and TalkBack on Android, checking labels, focus order, touch target size, dynamic text, contrast and error handling. Findings are recorded at the WCAG success criterion level in a draft ACR gap list, using WCAG 2.0 AA as the formal Section 508 baseline and noting where WCAG 2.1 or 2.2 AA adds a gap. The agency's 508 office makes the conformance determination.

Release Readiness

Can the agency ship an update next month? This step checks the SDK and target-API levels against current store requirements, whether the build still compiles on a current toolchain, who holds the signing keys and certificates, and whether the Apple and Google developer accounts belong to the agency. For workforce apps it checks distribution through the agency's MDM (Intune, Workspace ONE, Ivanti or equivalent) against SP 800-124 Rev. 2 device policies.

The Keep, Rebuild or Retire Memo

Not every app should survive. The memo asks whether the mission still needs native capabilities (offline work, camera or sensor capture, push, biometrics) or whether a mobile-friendly website would serve the same users under the 21st Century IDEA Act. It then recommends keep and remediate, rebuild, or retire, with a priced backlog for the first two. If the website is enough, the memo says so.

Deliverables

Deliverable	Format
Security findings by MASVS control, with an SP 800-163 vetting evidence gap list	PDF report and spreadsheet
Draft ACR gap list with manual assistive-technology evidence	Spreadsheet in VPAT criterion order, with screen recordings
Release-readiness checklist: SDK, toolchain, signing, accounts, MDM	Checklist and short memo
Evidence map to 800-53 controls for the ISSO	Spreadsheet
Keep, rebuild or retire memo with a priced remediation backlog	PDF memo and backlog in the agency's tracker

Where the Engagement Stops

The assessment stops at the backlog. Avalon offers the following as separate services: a penetration test (Vulnerability Assessment), the SSP or authorization package (SSP and ATO Process Facilitation), MDM operation (SaaS/laaS Implementation), and back-end work such as a server on Windows Server 2016 (end of support January 12, 2027) or a database on SQL Server 2016 (support ended July 14, 2026), which belongs to Application Modernization. A new cloud service behind the app is Cloud Native Development; open-source policy is Open-Source Technologies.

Evidence the Reviewers Can Use

Control or standard	What the assessment evidences
SA-11	Developer testing and evaluation: MASVS findings with static and dynamic test results
SA-15	Development process and tools: build toolchain, SDK currency and dependency state
IA-2, IA-5, IA-8	Authentication of agency and public users, and authenticator handling in the app
SC-8, SC-13, SC-28	Transmission protection, cryptography and protection of data stored on the device
AC-19, CM-7	Access control for mobile devices and least functionality in requested permissions
Section 508	Criterion-level manual test results for the named critical flows

The accurate way to state the value is narrow. The assessment tells the ISSO which pieces of vetting evidence exist and which do not, and tells the 508 coordinator where the app fails and why. A follow-on build or remediation produces the full vetting package and ACR. The government decides what to accept.

Accurate	Not accurate
MASVS-L1 findings as of the test date	The app is secure or approved
A draft ACR gap list from manual testing	The app is 508 certified
A vetting evidence gap list for the agency's process	The app passes vetting or receives an ATO
A release-readiness checklist	Apple or Google will approve the next update

How an Engagement Runs

Phase	Timing	What happens
0: Kickoff and access	1–2 weeks	Repository, build and test-distribution access issued; flows, devices and integrations named; dependency schedule signed
1: Assessment	3–5 weeks	Security verification, manual accessibility testing, release-readiness and authentication review
2: Memo and readout	Final week	Keep, rebuild or retire memo, priced backlog, five-business-day agency review, readout
Follow-on (separate, conditional)	Varies	Remediation, rebuild or sustainment, priced from the backlog

What the Agency Provides

- A product owner with decision authority, two to four hours a week, who can name the critical flows and approve the backlog.
- Read access to the source repository, build configuration and test distribution (TestFlight or internal test track), plus a current release build.
- A named device baseline and test devices, agency-furnished or through a device testing service the agency approves.
- Test accounts for every login path, a test environment and a named technical point of contact for each integration.
- Two to three hours a week from the ISSO and the 508 coordinator for findings review.
- Access to whoever holds the Apple and Google developer accounts and the MDM administrator. Account transfers can take weeks, so they are dated government-furnished dependencies. Agency-caused delays move the schedule day for day.

What Is Not Included

Included	Separate work
MASVS-L1 verification	A scoped penetration test under rules of engagement
Vetting evidence gap list	The vetting approval, the SSP or the ATO package
Draft ACR gap list for named flows	A final ACR, or agency-wide 508 remediation
MDM compatibility check	Operating the MDM platform or the device fleet
Integration review	Rebuilding the back end or its API layer
Agency-owned accounts and tools	Hardware, software or license resale
Unclassified apps	Classified networks or cleared environments

How Avalon Staffs It

Avalon takes one engagement at a time, works business hours, and works on unclassified apps only. Avalon's founder serves as delivery lead, with one named mobile technical lead hired for the engagement and a subcontracted Section 508 specialist. Avalon has no past federal engagements under this service. FAR 15.305 says an offeror without a record of past performance may not be evaluated favorably or unfavorably on that factor; what protects the program is a named team, a fixed price and a bounded scope. Avalon never serves as the independent tester of an app it built.

Requirement	How it is handled
Mobile technical lead	Named personnel whose certifications and investigation level match the agency's requirements, listed in the proposal
Section 508 specialist	Named, subcontracted specialist whose accessibility credentials match the agency's requirements, listed in the proposal
Civilian access	Public Trust investigation at the tier the agency requires, as a condition of the engagement
Devices and tools	Agency-furnished test devices or an agency-approved device service; MobSF runs in an agency-approved environment; Avalon hosts nothing
Accounts and code	Apple, Google and repository accounts stay in the agency's name; Avalon works under access the agency grants
Insurance and contract vehicles	Any coverage the solicitation requires is a condition of award; Avalon does not hold a GSA Schedule or a governmentwide contract today

Pricing and How to Buy

Engagement	Market-norm range	Avalon
One-app assessment, 3–5 weeks	\$35K–\$75K (discovery sprint band)	Firm fixed price, \$35K–\$65K; illustrative \$43K
Simple utility app build	\$150K–\$350K	Firm fixed price by milestone, scoped from the backlog
Standard mission or citizen app build	\$350K–\$900K	Firm fixed price by milestone, scoped from the backlog
Sustainment	\$8K–\$35K a month, or 15–25% of build cost a year	Monthly firm fixed price

The assessment is priced inside the market band for a discovery sprint because no separate band exists for assessing an existing app. It sits far under the \$350,000 simplified acquisition threshold and can be bought as an open-market purchase; 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. A simple utility build can also fit under the SAT. Larger work can be subcontracted to Avalon by a prime. Avalon does not hold a GSA Schedule or a governmentwide contract today, and it does not resell hardware, software or licenses.

Prices are fixed against a named app, platform count, critical-flow list, integration list and dated dependency schedule. There is no performance-based fee.

Illustration: One App, Two Platforms

The figures below are a planning illustration for one representative existing agency app on iOS and Android, with 8 critical flows, 3 back-end or identity integrations and a 4-week assessment. They are not a quote and not a result from any engagement.

Activity	Role	Hours
Kickoff and document review	Mobile lead	16

Activity	Role	Hours
MASVS-L1 verification (MobSF)	Mobile lead	80
Release readiness (SDK, signing, accounts, MDM)	Mobile lead	32
Authentication and integration review	Mobile lead	18
Report, decision memo and readout	Mobile lead	32
Manual assistive-technology testing	508 specialist	48
Draft ACR gap list	508 specialist	16
Delivery lead (0.25 FTE)	Founder	40
Total		282

What the Engagement Costs

Scope	Platforms, flows, integrations, weeks	Hours	Rate-band range	Planning fee
Lean	1, 6, 2, 3	180	\$21.6K–\$33.3K	\$35K
Base	2, 8, 3, 4	282	\$33.8K–\$52.2K	\$43K
Heavy	2, 12, 5, 5	328	\$39.4K–\$60.7K	\$50K

All hours are priced at the KB blended federal mobile rate band of \$120 to \$185 an hour, one rate card for every tier in this paper. The base case runs \$33.8K to \$52.2K with a \$43K planning fee at the midpoint. The lean case (one platform, 6 flows) runs \$21.6K to \$33.3K, below the \$35K floor, so it is priced at \$35K or folded into a larger scope. The heavy case (12 flows, 5 integrations) runs \$39.4K to \$60.7K, still inside the \$35K to \$65K quote range and the \$75K top of the market band. Every case sits far below the simplified acquisition threshold.

What Keeping the App Costs

Sustainment for annual OS updates, defects and patching runs 15 to 25 percent of build cost a year at market norms.

Build cost	Annual sustainment (15–25%)	Monthly equivalent
Simple utility app, \$150K	\$22.5K–\$37.5K	\$1.9K–\$3.1K
Simple to standard boundary, \$350K	\$52.5K–\$87.5K	\$4.4K–\$7.3K
Standard app, top of band, \$900K	\$135.0K–\$225.0K	\$11.2K–\$18.8K

For small apps the percentage falls below the \$8K floor of the monthly band, so small-app sustainment is quoted as a percentage. An app with no sustainment line will break at a future OS release.

Common Pitfalls

Pitfall	How to avoid it
Platform and device creep	Name the platforms, device baseline and critical flows in the statement of work
The phantom API	Name each integration with a technical contact and test environment; missing ones move the schedule
Overselling compliance	Deliver findings and evidence; the ISSO, AO and 508 office decide
Account and access lead times	Date developer-account, MDM and Public Trust steps as government-furnished dependencies
Treating 508 and security as end gates	Bring the ISSO and 508 coordinator into kickoff, not the readout
Push notifications that leak data	Check payloads during security verification
Incoherent rates across bundled proposals	One labor-rate card per proposal

Conclusion and Next Step

An agency app that nobody owns fails in predictable ways: it stops building, it fails screen reader users, and it reaches agency devices without vetting evidence. What most programs lack is one honest picture of the app's security, accessibility and release state, and a decision on whether it is worth keeping.

The natural first step is the fixed-fee assessment: one app, about three to five weeks, under the simplified acquisition threshold, ending in MASVS findings, a vetting evidence gap list, a draft ACR gap list, a release-readiness checklist, and a keep, rebuild or retire memo with a priced backlog. To discuss an app, contact Avalon Technology Services at contact@AvalonTechServices.com.

Appendices

Appendix A: Glossary

ACR

Accessibility Conformance Report: a criterion-by-criterion statement of accessibility conformance, usually in the VPAT template.

MASVS and MASTG

OWASP Mobile Application Security Verification Standard and Mobile Application Security Testing Guide. L1 is the baseline level.

MobSF

Mobile Security Framework: an open-source tool for static and dynamic testing of iOS and Android apps.

MDM

Mobile device management: the agency platform that enrolls devices, distributes apps and enforces device policy.

App vetting

The agency process, described in NIST SP 800-163 Rev. 1, for deciding whether an app is acceptable for use.

Derived PIV credential

A credential on a mobile device issued on the basis of an employee's PIV card (FIPS 201), as described in NIST SP 800-157.

Appendix B: Illustration Assumptions

All values are planning assumptions for one representative existing agency app. None is drawn from a specific agency, a real app or a completed engagement.

Assumption	Value	Basis
Scope	2 platforms, 8 critical flows, 3 integrations, 4 weeks	Planning assumption
Mobile lead hours	16 kickoff, 32 report, 40 and 16 per platform, 6 per integration	Planning assumption
508 specialist hours	3 per flow per platform, 16 ACR draft	Planning assumption
Delivery lead	0.25 FTE at 40 hours a week	Planning assumption
Rate	\$120–\$185 an hour, blended	KB federal mobile rate band
Price check	Base fee \$43K	Inside \$35K–\$65K quote and \$35K–\$75K band
Sustainment	15–25% of build cost a year	KB market norm

Appendix C: References

1. **U.S. Access Board**, *Section 508 standards, 36 CFR Part 1194*
<https://www.ecfr.gov/current/title-36/chapter-XI/part-1194>
2. **GSA**, *Section508.gov*
<https://www.section508.gov>
3. **W3C**, *Web Content Accessibility Guidelines (WCAG) 2.2*
<https://www.w3.org/TR/WCAG22/>
4. **U.S. Congress**, *H.R. 5759, 21st Century Integrated Digital Experience Act*
<https://www.congress.gov/bill/115th-congress/house-bill/5759>

5. **National Institute of Standards and Technology**, *SP 800-163 Rev. 1, Vetting the Security of Mobile Applications*
<https://csrc.nist.gov/pubs/sp/800/163/r1/final>
6. **National Institute of Standards and Technology**, *SP 800-124 Rev. 2, Guidelines for Managing the Security of Mobile Devices in the Enterprise*
<https://csrc.nist.gov/pubs/sp/800/124/r2/final>
7. **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>
8. **National Institute of Standards and Technology**, *SP 800-218, Secure Software Development Framework (SSDF) Version 1.1*
<https://csrc.nist.gov/pubs/sp/800/218/final>
9. **OWASP**, *Mobile Application Security (MASVS and MASTG)*
<https://mas.owasp.org>
10. **GSA**, *Login.gov developer documentation*
<https://developers.login.gov>
11. **Office of Management and Budget**, *M-26-05, Adopting a Risk-based Approach to Software and Hardware Security, January 23, 2026*
<https://www.whitehouse.gov/wp-content/uploads/2026/01/M-26-05-Adopting-a-Risk-based-Approach-to-Software-and-Hardware-Security.pdf>
12. **FedRAMP**, *FedRAMP program and 2026 Consolidated Rules*
<https://www.fedramp.gov>
13. **National Information Assurance Partnership**, *Protection Profiles*
<https://www.niap-ccevs.org>
14. **Acquisition.gov**, *FAR 15.305, Proposal evaluation*
<https://www.acquisition.gov/far/15.305>
15. **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/>