Remediation Proposal

Redacted iOS Application

Date: March 24, 2026

Audit Tier: Standard

Audit Fee: $3,000.00 (flat rate)

PIXELWRIGHT DIGITAL

Security Through Diligence

Proposal Version 1.0

Table of Contents

Executive Summary

TOTAL FINDINGS

26

ACTIONABLE FINDINGS

25

INFORMATIONAL ITEMS

0

ASSESSMENT ITEMS

1

ESTIMATED
TOTAL HOURS

24.75

ESTIMATED TOTAL COST

$3,094.00

Assessment Fee

1 items × $500.00 each = **$500.00**

Independent Adversarial Review

Independent review passes were used to challenge scan findings, validate evidence, and surface higher-risk logic issues that automated scanners can miss. This public sample preserves the deliverable structure while intentionally withholding internal tooling details.

Included review effort: $450.00

Remediation Line Items by Priority

Quick Fixes (under 0.5 hr)

ID	Title	CWE	Files Affected	Severity	Hours	Cost
PWD-2026-023	Force unwrapping should be avoided	CWE-476	App/Source-07.swift	Medium	0.25	$31.25
	Related to: PWD-2026-025, PWD-2026-021, PWD-2026-022, PWD-2026-024					
PWD-2026-011	DataStore Silently Swallows Persistence Errors Causing Silent Data Loss	CWE-755	App/Source-03.swift	Medium	0.25	$31.25
	Related to: PWD-2026-010, PWD-2026-012, PWD-2026-013, PWD-2026-014, PWD-2026-015					
PWD-2026-009	Force unwrap is a crash risk in production. Use optional binding or nil coalescing.	CWE-476	App/Source-03.swift App/Source-07.swift	Low	0.5	$62.50
Quick Fixes Subtotal					**1.0**	**$125.00**

Moderate Fixes (0.5–2 hr)

ID	Title	CWE	Files Affected	Severity	Hours	Cost
PWD-2026-092	Insecure Storage of Third-Party API Key in UserDefaults	CWE-312	App/Source-07.swift	High	0.75	$93.75
PWD-2026-093	Sensitive data stored in UserDefaults. Use Keychain instead.	CWE-312	App/Source-10.swift	High	1.0	$125.00
	Related to: PWD-2026-026, PWD-2026-027					
PWD-2026-094	Sensitive User Data in Unprotected JSON Files Exposed via Device Backups	CWE-312	App/Source-03.swift	Medium	0.5	$62.50
PWD-2026-037	File should contain 500 lines or less: currently contains 554	—	App/Source-01.swift	Medium	0.5	$62.50
PWD-2026-041	File should contain 500 lines or less: currently contains 565	—	App/Source-02.swift	Medium	0.5	$62.50

ID	Title	CWE	Files Affected	Severity	Hours	Cost
PWD-2026-042	Class body should span 300 lines or less excluding comments and whitespace: currently spans 339 line	—	App/Source-03.swift	Medium	0.5	$62.50
PWD-2026-045	File should contain 500 lines or less: currently contains 518	—	App/Source-03.swift	Medium	0.5	$62.50
PWD-2026-047	Struct body should span 300 lines or less excluding comments and whitespace: currently spans 319 lin	—	App/Source-07.swift	Medium	0.5	$62.50
PWD-2026-050	File should contain 500 lines or less: currently contains 622	—	App/Source-07.swift	Medium	0.5	$62.50

ID	Title	CWE	Files Affected	Severity	Hours	Cost
PWD-2026-081	Struct body should span 500 lines or less excluding comments and whitespace: currently spans 604 lin	—	App/Source-15.swift	Medium	0.5	$62.50
PWD-2026-083	File should contain 1000 lines or less: currently contains 1267	—	App/Source-15.swift	Medium	0.5	$62.50
PWD-2026-085	Struct body should span 300 lines or less excluding comments and whitespace: currently spans 363 lin	—	App/Source-17.swift	Medium	0.5	$62.50
PWD-2026-088	File should contain 1000 lines or less: currently contains 1050	—	App/Source-17.swift	Medium	0.5	$62.50

ID	Title	CWE	Files Affected	Severity	Hours	Cost
PWD-2026-089	Struct body should span 300 lines or less excluding comments and whitespace: currently spans 427 lin	—	App/Source-18.swift	Medium	0.5	$62.50
PWD-2026-091	File should contain 500 lines or less: currently contains 669	—	App/Source-18.swift	Medium	0.5	$62.50
PWD-2026-034	Sensitive Data Stored in UserDefaults	CWE-921	Docs/Document-01.md	Low	0.5	$62.50
Moderate Fixes Subtotal					**8.75**	**$1,093.75**

Complex Fixes (2–6 hr)

ID	Title	CWE	Files Affected	Severity	Hours	Cost
PWD-2026-036	Prompt Injection Via Unsanitized User Content in AI Prompts	CWE-77	App/Source-01.swift	High	2.25	$281.25

ID	Title	CWE	Files Affected	Severity	Hours	Cost
PWD-2026-077	Monetization and Quota System Bypassed via User-Accessible "Beta Mode"	CWE-840	App/Source-14.swift	High	2.25	$281.25
PWD-2026-078	Subscription Tier and Beta Mode Bypass via UserDefaults Manipulation	CWE-807	App/Source-14.swift	High	2.25	$281.25
PWD-2026-040	Function body should span 50 lines or less excluding comments and whitespace: currently spans 55 lin	—	App/Source-02.swift	Medium	2.75	$343.75
PWD-2026-044	Function body should span 50 lines or less excluding comments and whitespace: currently spans 51 lin	—	App/Source-03.swift	Medium	2.75	$343.75
PWD-2026-087	Optional should be implicitly initialized without nil	—	App/Source-17.swift	Medium	2.75	$343.75
Complex Fixes Subtotal					**15.0**	**$1,875.00**

Findings Requiring Assessment

The following findings require a deeper review before we can provide a fixed estimate. Each scoping assessment is $500.00, credited toward the remediation if you proceed. Final remediation costs for assessed items typically range $500-$2,000 per finding.

ID	Title	CWE	Files Affected	Why Assessment Needed	Fee
PWD-2026-010	Force try crashes on any error. Use do-catch or try? in production code.	CWE-755	App/Source-01.swift App/Source-02.swift +12 more	*14+ files affected*	**$500.00**
Assessment Fees Subtotal (1 items)					**$500.00**

Estimated Cost Summary

Standard Audit (flat fee)	**$3,000.00**

REMEDIATION (OPTIONAL)

Quick Fixes (3 items)	**$125.00**
Moderate Fixes (16 items)	**$1,093.75**
Complex Fixes (6 items)	**$1,875.00**
Assessment Fees (1 × $500.00)	**$500.00**
Discovery Allowance (15% — 3.75 hr)	**$469.00**

Independent Adversarial Review	**$450.00**

ESTIMATED REMEDIATION TOTAL	**$4,513.00**

Total Engagement Cost (Audit + Remediation)	**$7,513.00**

Note: *Estimates are based on the automated analysis in your audit report and may be refined after we review your codebase in detail. Items marked "Needs Assessment" require a brief scoping conversation before we can quote a fixed price. The Discovery*

Allowance covers additional findings identified during remediation work — if unused, it is not billed.

Ready to move forward?

Reply to this report and let us know which items you'd like us to address. We can start with the quick fixes and work through the list at your pace, or tackle everything as a single engagement. No commitment required for assessment-tier items until after the scoping call.

What You Receive

Typical remediation engagements include the following deliverables, adjusted as needed for the agreed scope and technical constraints of the codebase.

DELIVERABLE

Remediation Branch

A branch or patch set containing the agreed remediation work, organized for client review and integration.

DELIVERABLE

Verification Summary

A concise summary of what was re-checked after remediation and the resulting status of the addressed findings.

DELIVERABLE

Regression Coverage

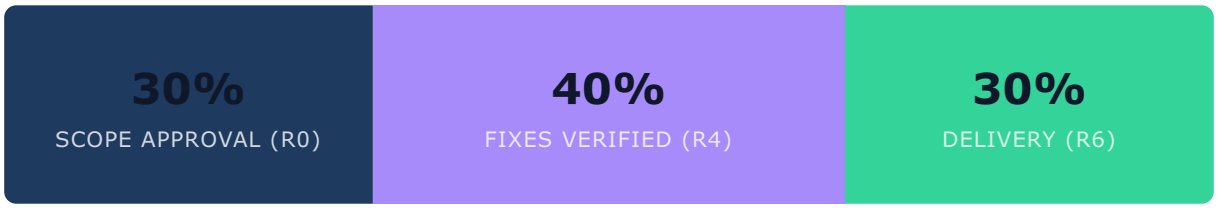
Targeted test updates or verification steps where automated regression coverage is part of the agreed remediation scope.

DELIVERABLE

Automation Updates

CI or scanning workflow changes, when requested, to help keep remediated issues from reappearing unnoticed.

Engagement Timeline



Milestone	Payment	What Happens
Scope Approval	30%	We review the findings, confirm scope, and align the remediation plan before implementation begins.
Fixes Verified	40%	Agreed fixes are implemented, reviewed, and re-checked against the relevant validation steps. You review the resulting branch or patch set.
Delivery	30%	You receive the agreed remediation deliverables, verification summary, and 2 hours of post-delivery support.

Continuous Protection

Fixing today's findings is the first step. Your codebase changes every week — new code, new dependencies, new attack vectors. A quarterly security retainer keeps your posture current without the overhead of a full re-engagement each time.

Quarterly Security Retainer

INCLUDED

- Full re-scan with the same tool suite
- Delta report (what's new, what regressed)
- Updated verification summary
- CI or scanning workflow updates when in scope

WHY IT MATTERS

- Catch regressions before they ship
- Maintain compliance documentation
- Track security posture over time
- Priority access for new findings

Retainer pricing is discussed after the initial remediation is complete, based on codebase size and change velocity. There is no commitment required at this stage.

Disclaimer

This proposal is based on the findings identified during the associated code audit. Estimates reflect the effort required to remediate the specific issues documented and may be revised after detailed review of the codebase. Actual effort may vary based on code complexity, dependencies, and testing requirements discovered during implementation.

This proposal is valid for 30 days from the date shown on the cover page. After this period, estimates may need to be revised to reflect changes in the codebase or updated security advisories.

This public sample has been redacted for portfolio and marketing use. Project identity and proprietary implementation details have been intentionally withheld. Pixelwright Digital retains all rights to its methodology, tooling, and processes described herein. Acceptance of this proposal does not guarantee elimination of all security risk; it covers only the remediation work explicitly included in the agreed scope for the listed findings.