OVERVIEW

WS05
3–4 weeks
Forge Honor Assurance

SBA U.S. Small Business Administration
VETERAN-OWNED CERTIFIED

Auth and Data Exposure Remediation Sprint

Representative sample engagement for closing audit findings with evidence.

ENGAGEMENT FIT

Engineering teams that already know what is wrong and need fixes landed, tested, and documented.

SCENARIO

A product team has a short list of security findings from an internal review and a customer deadline. The highest-risk issues involve authorization checks, overly broad data returned from an API, missing regression tests, and inconsistent cloud configuration. The team needs practical implementation support.

CONSTRAINTS

- The buyer wants fixes in the existing codebase rather than a generic advisory report.
- Engineering ownership remains with the buyer, but Forge Honor Assurance can pair, review, or implement scoped patches.
- The sprint must produce verification evidence suitable for customer follow-up.
- Residual risk must be documented when a finding cannot be fully closed within the sprint.

This is a representative composite report showing the type of work product Forge Honor Assurance can provide. It is not a client case study.

REPORT DATA

SAMPLE ID
WS05

CATEGORY
Remediation Sprint

TIMEFRAME
3-4 weeks

BEST FOR
Engineering teams that already know what is wrong and need fixes landed, tested, and documented.

USE NOTE

Representative composite sample. No client PII, proprietary environment detail, or confidential facts are included.

Final scopes, controls, deliverables, and timelines are confirmed in writing per engagement.

DELIVERY PLAN

WS05
3–4 weeks
Forge Honor Assurance

SBA U.S. Small Business Administration
VETERAN-OWNED CERTIFIED

Scope and Delivery Plan

A practical work plan with written scope, explicit boundaries, and deliverables the buyer can inspect.

SCOPE

- Convert findings into a sequenced remediation backlog with owners and acceptance criteria.
- Patch or pair on authorization, data-minimization, logging, dependency, and cloud-hardening issues.
- Add regression tests or verification checks for the fixed behavior.
- Retest closed items and collect evidence.
- Produce a verification memo and residual-risk notes.

TIMELINE

PHASE	FOCUS	EXPECTED WORK
Days 1–2	Backlog and access	Review findings, confirm acceptance criteria, agree repo access, and select sprint scope.
Days 3–8	Implementation	Land patches or pair with engineers on highest-risk items.
Days 9–12	Tests and review	Add regression tests, review changes, and verify no obvious breakage.
Days 13–15	Retest	Retest closed findings and collect screenshots, logs, requests, or test evidence.
Optional week 4	Residual work	Address remaining medium-risk items and prepare customer-ready memo.

DELIVERABLES

- **Remediation backlog: Finding-to-task mapping with owner, priority, acceptance criteria, and target date.**
- **Patches or pairing: Scoped code/config changes or direct engineering support.**
- **Test evidence: Regression tests, verification requests, screenshots, or logs as appropriate.**
- **Verification memo: Plain-language closure notes for leadership, customer, or vendor security team.**
- **Residual-risk register: Items not fully closed, reason, compensating controls, and recommended next step.**

Sample remediation ticket

A good sprint turns vague findings into concrete acceptance criteria.

FIELD	EXAMPLE
Finding	API returns full customer object when summary fields are sufficient.
Fix	Create response DTO with approved fields and update handler to use server-side authorization context.
Acceptance criteria	Cross-tenant request returns 403; summary endpoint returns no billing or private contact fields.
Evidence	Unit test, integration test, before/after response sample, and log screenshot.
Owner	FHA pairs with API owner; buyer approves PR.

HANDOFF

- **The buyer receives code/config changes, test notes, closure evidence, and a customer-ready verification memo.**
- **The sprint is designed to close the highest-risk items first, not boil the ocean.**
- **Future phases can address remaining medium/low findings, deeper architecture changes, or recurring review cadence.**

SAMPLE OUTPUT

WS05
3–4 weeks
Forge Honor Assurance

Sample verification memo excerpt

The final memo should be useful to customers without exposing sensitive internals.

FINDING	STATUS	VERIFICATION
F-01 Tenant authorization	Closed	Server-side tenant context enforced; cross-tenant regression test passes.
F-02 Excessive API fields	Closed	Response schema reduced to approved fields; integration test added.
F-03 Secret rotation	Closed	Staging secret rotated and moved to managed secret store.
F-04 Legacy admin role	Residual	Role remains for two users with compensating monitoring until Q3 migration.

BOUNDARIES

- **Implementation depends on repo access, environment access, and buyer approval flow.**
- **Forge Honor Assurance will not bypass change-control or production approval processes.**
- **A verification memo is not a compliance certification or guarantee of future security.**