SLIDE 1 · COVER

ShieldSpec

Productized SCIF scope intelligence and execution readiness.

Founder: Alex Potter | Stage: Packaging + pilots | Role: Portfolio force multiplier

SLIDE 2 · PROBLEM

Scope quality breaks secure-project execution

- Missing access constraints and sequencing realities
- Underestimated compliance/site-control requirements
- Poor handoff from planning to field execution

Impact: change orders, schedule slippage, and compliance exposure in high-stakes environments.

SLIDE 3 · SOLUTION

Scope preflight and risk-ready work packages

1) Scope Preflight Audit

Detect delivery risk before mobilization.

2) Execution Readiness Package

Standardized, field-usable work package.

3) Risk Flags + Checklist

Control points aligned to secure facility realities.

Outcome:

Higher predictability, lower rework, cleaner closeout.

SLIDE 4 · BUSINESS MODEL + GTM

Revenue Model

- Fixed-fee scope audit packages
- Tiered readiness engagements
- Enterprise retainer for portfolio-level support

Go-to-Market

- Sell into existing secure-project relationships
- Bundle with ClearedConnect execution work
- Expand through measurable delay/rework reduction

SLIDE 5 · STRATEGIC FIT + MOAT

Why It Wins

- Domain-native judgment from classified field experience
- Productized service in a trust-constrained niche
- Direct impact on downstream margin and execution quality

Portfolio Flywheel

- ShieldSpec improves scope quality
- ClearedConnect improves staffing and execution
- Together they compound trust, data, and repeat demand

SLIDE 6 · ASK + MILESTONES

Capital ask to productize and scale

Use of funds: standardized delivery templates, sales assets, and software-assisted scope analysis layer.

12-Month Milestones

- Predictable productized pricing
- 10+ paid scope engagements
- Measured reduction in rework/delay risk
- Integrated pipeline with ClearedConnect

Investor Outcome

A differentiated, defensible wedge into SCIF execution with strong cross-sell and platform adjacency.

SECURITY & CONFIDENTIALITY

Sensitive information protection is core to delivery

- Emails, blueprints, and package artifacts handled under strict confidentiality
- Need-to-know coordination and least-privilege access handling
- No external sharing without explicit client authorization