

AGORA

Post-Quantum Security Audit Pack

Program: /home/king_d/solana/testing/jito-restaking

Scan date: 2026-05-24T04:39:34.800044798+00:00

Tool: Pinpoint SPECTRE 1.2.2

CONFIDENTIAL. For authorised recipients only.

Executive Summary

Total findings: 27

Cryptographic components inventoried (CBOM 1.6): 0

Findings by rule: CA-001=0, CA-002=0, CA-003=0, CA-004=0

CA-005: not applicable. PDAs are quantum-safe by construction.

Findings

No findings emitted by the post-quantum rule pack.

NIST IR 8547 Traceability Matrix

Maps each audit-pack section to a NIST IR 8547 post-quantum transition phase.

Phase	Rule(s)	Finding Count
Inventory	CA-001	0
Risk Prioritisation	CA-002, CA-003, CA-004	0
Hybrid Deployment	(no rules at this release)	n/a
Full Migration	(no rules at this release)	n/a

Hybrid Deployment and Full Migration are documented for framework completeness.

No CA rule fires for those phases at this release. Coverage expands in Tier 2.

Methodology

Pre-pass: Anchor expand subprocess invoked before tree-sitter walks source.

Expanded output is cached per program hash to avoid redundant re-expansion.

OtterSec downstream framing: CA-003 cross-program assumption findings surface migration cascade complexity following OtterSec's CPI-trust analysis framework.

CA-005 dropped: PDAs are quantum-safe by construction. Off-curve points derived via SHA-256 have no Ed25519 private key, so the Grover speedup falls beyond the attack horizon. Confirmed with Jump Crypto and Helius.

CA-004 is inventory and exposure only. It does not prescribe a hybrid Falcon co-signer. Protocol-layer migration (address format, ZK proof of Ed25519 seed) is owned by Anza and Firedancer, not by individual program developers.

Rule pack: pinpoint-rules-pq v0.1.0. CBOM format: CycloneDX 1.6.

PDF renderer: printpdf (pure Rust, no system library dependency).