Critical Dependency Update Plan

Current Vulnerabilities Identified

🔴 CRITICAL - Cryptographic Libraries

1. **curve25519-dalek 3.2.1 → 4.1.3+**
   - **Vulnerability**: Timing variability in `Scalar29::sub`/`Scalar52::sub`
   - **Impact**: Potential timing attacks
   - **Fix**: Upgrade to >=4.1.3
2. **ed25519-dalek 1.0.1 → 2.0.0+**
   - **Vulnerability**: Double Public Key Signing Function Oracle Attack
   - **Impact**: Signature forgery attacks
   - **Fix**: Upgrade to >=2.0.0

⚠ WARNINGS - Unmaintained Packages

3. **atty 0.2.14 → is-terminal 0.4.16+**
   - **Status**: Unmaintained
   - **Impact**: No security updates
   - **Fix**: Replace with maintained alternative
4. **derivative 2.2.0 → Latest maintained version**
   - **Status**: Unmaintained
   - **Impact**: No security updates
   - **Fix**: Update to latest version
5. **paste 1.0.15 → Latest maintained version**
   - **Status**: Unmaintained
   - **Impact**: No security updates
   - **Fix**: Update to latest version

⚠ UNSOUND - Parsing Library

6. **borsh 0.9.3 → 1.0.0+**
   - **Vulnerability**: Unsound parsing with ZST
   - **Impact**: Memory safety issues
   - **Fix**: Upgrade to >=1.0.0

Update Strategy

Phase 1: Anchor Framework Update

The vulnerabilities are in transitive dependencies through Anchor. We need to:

1. Update to latest Anchor version that includes fixed dependencies
2. Check compatibility with our code changes
3. Test thoroughly

Phase 2: Direct Dependency Override

If Anchor doesn't include the latest fixes, we'll override specific versions in Cargo.toml.

Phase 3: Security Validation

1. Run cargo audit after updates
2. Verify no new vulnerabilities introduced
3. Test all functionality

Implementation Steps

Step 1: Check Latest Anchor Version

```
cargo search anchor-lang
cargo search anchor-spl
```

Step 2: Update Cargo.toml

```
[dependencies]
anchor-lang = "0.30.2"  # Latest version
anchor-spl = "0.30.2"   # Latest version

# Override vulnerable dependencies if needed
[patch.crates-io]
curve25519-dalek = "4.1.3"
ed25519-dalek = "2.2.0"
borsh = "1.0.0"
```

Step 3: Test Compatibility

1. Build the project
2. Run tests
3. Verify security fixes still work

Step 4: Security Validation

1. Run cargo audit
2. Verify no critical vulnerabilities remain
3. Document any remaining issues

Expected Timeline

- **Phase 1**: 1-2 days (Anchor update and testing)
- **Phase 2**: 1-2 days (Direct overrides if needed)
- **Phase 3**: 1 day (Security validation)
- **Total**: 3-5 days

Risk Assessment

- **Low Risk**: Anchor updates are generally backward compatible
- **Medium Risk**: Direct dependency overrides may cause conflicts
- **Mitigation**: Thorough testing at each step

Rollback Plan

- Keep current working version in git
- Test each update incrementally
- Revert if critical issues found