# Sky: Solana Bridge Migration

## Security Review

Cantina Managed review by:

**M4rio.eth**, Lead Security Researcher

**Xmxanuel**, Lead Security Researcher

November 12, 2025

# Contents

# 1 Introduction

## 1.1 About Cantina

Cantina is a security services marketplace that connects top security researchers and solutions with clients. Learn more at cantina.xyz

## 1.2 Disclaimer

Cantina Managed provides a detailed evaluation of the security posture of the code at a particular moment based on the information available at the time of the review. While Cantina Managed endeavors to identify and disclose all potential security issues, it cannot guarantee that every vulnerability will be detected or that the code will be entirely secure against all possible attacks. The assessment is conducted based on the specific commit and version of the code provided. Any subsequent modifications to the code may introduce new vulnerabilities that were absent during the initial review. Therefore, any changes made to the code require a new security review to ensure that the code remains secure. Please be advised that the Cantina Managed security review is not a replacement for continuous security measures such as penetration testing, vulnerability scanning, and regular code reviews.

## 1.3 Risk assessment

| **Severity level** | **Impact: High** | **Impact: Medium** | **Impact: Low** |
|---|---|---|---|
| **Likelihood: high** | Critical | High | Medium |
| **Likelihood: medium** | High | Medium | Low |
| **Likelihood: low** | Medium | Low | Low |

### 1.3.1 Severity Classification

The severity of security issues found during the security review is categorized based on the above table. Critical findings have a high likelihood of being exploited and must be addressed immediately. High findings are almost certain to occur, easy to perform, or not easy but highly incentivized thus must be fixed as soon as possible.

Medium findings are conditionally possible or incentivized but are still relatively likely to occur and should be addressed. Low findings are a rare combination of circumstances to exploit, or offer little to no incentive to exploit but are recommended to be addressed.

Lastly, some findings might represent objective improvements that should be addressed but do not impact the project's overall security (Gas and Informational findings).

# 2 Security Review Summary

Sky Protocol is a decentralised protocol developed around the USDS stablecoin.

From Nov 5th to Nov 11th the Cantina team conducted a review of v2 on commit hash d3409c29. The team identified a total of **2** issues:

**Issues Found**

| Severity | Count | Fixed | Acknowledged |
|---|---|---|---|
| Critical Risk | 0 | 0 | 0 |
| High Risk | 0 | 0 | 0 |
| Medium Risk | 1 | 1 | 0 |
| Low Risk | 1 | 1 | 0 |
| Gas Optimizations | 0 | 0 | 0 |
| Informational | 0 | 0 | 0 |
| **Total** | **2** | **2** | **0** |

## 2.1 Cantina Managed Team Statement

This section documents the verification procedures performed to validate the correctness of the USDS bridge migration from Wormhole to LayerZero on Solana and Ethereum, including the new governance framework.

All verification checks were performed prior to deployment to ensure system integrity and correctness.

**1. Repository and Code Verification**

**1.1 Commit Hash Verification**

**LZ EVM Token Bridge (SkyOFTAdapter)**

- Repository: `sky-ecosystem/sky-oapp-oft`
- Verified Commit: `b044009`
- Status: ✓ Matches audited version

**LZ Solana Token Bridge (`oft` program)**

- Repository: `sky-ecosystem/sky-oapp-oft`
- Verified Commit: `8d7309d60caa1194cd8be67e26f3b8a669cc096a`
- Audited Version: `b5c6ef5`
- Status: ✓ Code identical to audited version

**LZ EVM Governance OApp (Sender/Receiver)**

- Repository: `sky-ecosystem/sky-oapp-oft`
- Verified Commit: `03fa6e8609227440f04bf6f4bbbef61dc87218e7`
- Status: ✓ Matches audited version

**LZ Governance Relays (L1GovernanceRelay, L2GovernanceRelay)**

- Repository: `sky-ecosystem/lz-governance-relay`
- Verified Commit: `d3e3df4`
- Status: ✓ Matches audited version

**LZ Solana Governance Program**

- Repository: `sky-ecosystem/sky-oapp-oft`
- Verified Commit: `8d7309d60caa1194cd8be67e26f3b8a669cc096a`

- Audited Version: `c9db37d`
- Status: ✓ Code identical to audited version

**NTT Migration (EVM)**

- Repository: `sky-ecosystem/sky-ntt-migration`
- Verified Commit: `722c14f4b9cf6073367354bc78bd60fa49b871e6`
- Audited Version: `832781e`
- Status: ✓ Code identical to audited version

**NTT Migration (Solana)**

- Repository: `sky-ecosystem/sky-ntt-migration`
- Verified Commit: `722c14f4b9cf6073367354bc78bd60fa49b871e6`
- Audited Version: `626962a`
- Status: ✓ Code identical to audited version

**Solana Cross-chain Payload Tooling**

- Repository: `keel-fi/crosschain-gov-solana-spell-payloads`
- Initial Commit: `ad99254`
- Final Version: `11baa180d4ad6c7579c69c8c0168e17cb73bb6ed`
- Status: ✓ Validated with mainnet values

**L1 Spell**

- Repository: `sky-ecosystem/wh-lz-migration`
- Verified Commit: `1739787`
- Status: ✓ Verified

**InFlight Checker Scripts**

- Repository: `sky-ecosystem/sky-ntt-migration`
- PR: `#16`
- Commit: `4ef3d241035da5438c95daf89004deb4325e6dda`
- Status: ✓ Verified

## 2. Ethereum Mainnet Verification

### 2.1 Core Contract Deployments

**USDS Token**

- Address: `0xdc035d45d973e3ec169d2276ddab16f1e407384f`
- Status: ✓ Existing contract verified

**MCD_PAUSE_PROXY**

- Address: `0xbe8e3e3618f7474f8cb1d074a26affef007e98fb`
- Status: ✓ Existing contract verified

**L1GovernanceRelay**

- Address: `0x2beBFe397D497b66cB14461cB6ee467b4C3B7D61`
- Bytecode Verification: ✓ Partial match (creation code)
- Version: ✓ Same as Cantina Review
- Ward Status: ✓ PauseProxy is ward
- Configuration:

    - `l1Oapp` pointing to zero, correct value later: ✓ Verified
    - `lzToken` pointing to zoro, correct value later: ✓ Verified

**GovernanceOAppSender**

- Address: `0x27FC1DD771817b53bE48Dc28789533BEa53C9CCA`
- Bytecode Verification: ✓ Partial match (creation code)
- Version: ✓ Same as Cantina Review
- Configuration Checks:
    - Owner: ✓ Set to PauseProxy (`0xBE8E3e3618f7474F8cB1d074A26afFef007E98FB`)
    - Endpoint: ✓ `0x1a44076050125825900e736c501f859c50fE728c` (LayerZero EndpointV2)
    - Peer (EID=30168): ✓ `0x75b81a4430dee7012ff31d58540835ccc89a18d1fc0522bc95df16ecd50efc32`
        * Converts to Base58: `8vXXGiaXFrKFUDw21H5Z57ex552Lh8WP9rVd2ktzmcCy` (LZ Gov PDA)
    - Enforced Options: ✓ No enforced options (as expected)
    - canCallTarget: ✓ Configuration validated

**SkyOFTAdapter**

- Address: `0x1e1D42781FC170EF9da004Fb735f56F0276d01B8`
- Bytecode Verification: ✓ Partial match (creation & runtime code)
- Version: ✓ Same as Cantina Review (main branch)
- Configuration Checks:
    - Owner: ✓ PauseProxy
    - Token: ✓ USDS (`0xdC035D45d973E3EC169d2276DDab16f1e407384F`)
    - Endpoint: ✓ Ethereum Mainnet Endpoint V2
    - Delegate: ✓ PauseProxy
    - Peer (EID=30168): ✓ `0x9825dc0cbeaf22836931c00cb891592f0a96d0dc6a65a4c67992b01e0db8d122`
        * Converts to Base58: `BEvTHkTyXooyaJzP8egDUC7WQK8cyRrq5WvERZNWhuah` (OFT Store PDA)
    - Pauser: ✓ Safe Multisig (`0x38d1114b4ce3e079cc0f627df6ac2776b5887776`)
    - Shared Decimals: ✓ 6
    - Default Fee: ✓ 0 bps
    - Rate Limits: ✓ Initially set to 0 (as expected for pre-migration state)

**Enforced Options Configuration**

- Message Type 1 (SEND):
    - Type: 3 (Options V3)
    - Kind: 0x01 (LZ_RECEIVE)
    - Length: 33 bytes
    - Mode: 1
    - Value: 0
    - Gas: 200,000 compute units
    - Extra Value: 0
    - Extra Gas: 2,039,280

    - Status: ✓ Verified

- Message Type 2 (SEND_AND_CALL):
    - Same configuration as Type 1
    - Status: ✓ Verified

### 2.2 NTT Manager Implementation

#### Current NTT Manager Implementation

- Address: `0x37c618755832ef5ca44fa88bf1ccdce46f30b479`
- Status: ✓ Existing contract verified

#### New NTT Manager Implementation

- Address: `0xD4DD90bAC23E2a1470681E7cAfFD381FE44c3430`
- Bytecode Verification: ✓ Same as Cantina Review
- Immutable Parameters Verified:
    - Token: ✓ `0xdC035D45d973E3EC169d2276DDab16f1e407384F` (USDS)
    - Mode: ✓ 0
    - Chain ID: ✓ 2
    - Rate Limit Duration: ✓ 86400 (24 hours)
- Compilation Settings:
    - viaIR: ✓ true
    - TransceiverStructs library: ✓ Correct address

#### NTT Manager Proxy

- Address: `0x7d4958454a3f520bDA8be764d06591B054B0bf33`
- Status: ✓ Existing contract verified

## 3. Solana Mainnet Verification

### 3.1 USDS Token Accounts

#### USDS Mint

- Address: `USDSwr9ApdHk5bvJKMjzff41FfuX8bSxdKcR81vTwcA`
- Status: ✓ Existing program verified
- Current Authorities (Pre-Migration):
    - Mint Authority: `Bjui9tuxKGsiF5FDwosfUsRUXg9RZCKidbThfm6CRtRt` (NTT Token Authority PDA)
    - Freeze Authority: `66xDajRZ7MTrgePf27NdugVwDBFhKCCY9EYZ7B9CdDWj` (Wormhole Sky Governance Authority)
    - Metadata Update Authority: `66xDajRZ7MTrgePf27NdugVwDBFhKCCY9EYZ7B9CdDWj` (Wormhole Sky Governance Authority)

#### USDS Token Account (Escrow)

- Address: `8GVwe5nYwqkC9udmj1LsGMD5pYDq2ZtKH9YNrzWzV3Z2`
- Status: ✓ Verified as OFT Escrow

### 3.2 LayerZero Governance Program

#### LZ Governance Program

- Program ID: `SKYGRikJcGSa3jC5HDyzDrVsmkCk3e5SqAurycny8PW`
- Verification: ✓ Matches commit `8d7309d60caa1194cd8be67e26f3b8a669cc096a`

- Verification Method: `solana-verify verify-from-repo` with commit hash validation

### Governance PDA (params.id == 0)

- Address: `8vXXGiaXFrKFUDw21H5Z57ex552Lh8WP9rVd2ktzmcCy`
- Derivation: ✓ Verified from seeds: `[Governance, id=0]`
- Bump: 251
- Admin: `AYPtjx4Hc8us1ikULUedkmZ3wtiD6tmL7gK3qe4V3oHt` (LZ CPI Authority PDA)

### LZ CPI_Authority PDA

- Address: `AYPtjx4Hc8us1ikULUedkmZ3wtiD6tmL7gK3qe4V3oHt`
- Derivation: ✓ Verified from seeds: `[CpiAuthority, Gov PDA, src_eid=30101, origin_caller]`
- Origin Caller: `0x0000000000000000000000002bebfe397d497b66cb14461cb6ee467b4c3b7d61`
  - Corresponds to: `0x2beBFe397D497b66cB14461cB6ee467b4C3B7D61` (L1GovernanceRelay)
- Purpose: Cross-chain governance authority controlled by PauseProxy

### LZ Receive Types v2 Accounts PDA

- Address: `4w217yJEDanxz6n3fXWTWt9NZCWed2GabQhfwpdqctTG`
- Derivation: ✓ Verified from seeds: `[LzReceiveTypes, Gov PDA]`

### LZ Governance Remote PDA (Peer)

- Address: `J2JDYYdWkQz7Y2YPVFiR2EYaMLeH6FgYsjdgiVuPcPgA`
- Derivation: ✓ Verified from seeds: `[Remote, Gov PDA, eid=30101]`
- Peer Address (hex32): `0x00000000000000000000000027fc1dd771817b53be48dc28789533bea53c9cca`
  - Corresponds to: `0x27FC1DD771817b53bE48Dc28789533BEa53C9CCA` (GovernanceOAppSender)

### LZ OApp Registry

- Address: `DbTxk1FeZtR5YqaCLc5cLrMq4aPYpcnyPACrwUC1yBMn`
- Derivation: ✓ Verified from LZ Endpoint seeds: `[OApp, Gov PDA]`
- Endpoint Program: `76y77prsiCMvXMjuoZ5VRrhG5qYBrUMYTE5WgHqgjEn6`
- Delegate: ✓ Verified as `AYPtjx4Hc8us1ikULUedkmZ3wtiD6tmL7gK3qe4V3oHt` (LZ CPI Authority PDA)

### Governance Program Configuration

- Upgrade Authority: ✓ Verified as `AYPtjx4Hc8us1ikULUedkmZ3wtiD6tmL7gK3qe4V3oHt` (LZ CPI Authority PDA)
- Governance Admin: ✓ Verified as `AYPtjx4Hc8us1ikULUedkmZ3wtiD6tmL7gK3qe4V3oHt` (LZ CPI Authority PDA)
- Delegate: ✓ Verified as `AYPtjx4Hc8us1ikULUedkmZ3wtiD6tmL7gK3qe4V3oHt` (LZ CPI Authority PDA)
- Enforced Options: ✓ No enforced options set (as expected)
- ALTs (Address Lookup Tables): ✓ No ALTs configured

## 3.3 LayerZero OFT Program

### Sky OFT App (oft program)

- Program ID: `SKYTAiJRkgexqQqFoqhXdCANyfziwrVrzjhBaCzdbKW`
- Verification: ✓ Matches commit `8d7309d60caa1194cd8be67e26f3b8a669cc096a`
- Verification Method: `solana-verify verify-from-repo` with commit hash validation

### OFT Store PDA

- Address: `BEvTHkTyXooyaJzP8egDUC7WQK8cyRrq5WvERZNWhuah`
- Derivation: ✓ Verified from seeds: `[OFT, token_escrow]`
- Configuration Verified:
  - OFT Type Tag: ✓ 0 (Native)
  - LD2SD Rate: ✓ 1
  - Token Mint: ✓ `USDSwr9ApdHk5bvJKMjzff41FfuX8bSxdKcR81vTwcA` (USDS)
  - Token Escrow: ✓ `8GVwe5nYwqkC9udmj1LsGMD5pYDq2ZtKH9YNrzWzV3Z2`
  - Endpoint Program: ✓ `76y77prsiCMvXMjuoZ5VRrhG5qYBrUMYTE5WgHqgjEn6` (LZ EndpointV2)
  - Bump: ✓ 255
  - TVL: ✓ 0
  - Admin: ✓ `AYPtjx4Hc8us1ikULUedkmZ3wtiD6tmL7gK3qe4V3oHt` (LZ CPI Authority PDA)
  - Default Fee BPS: ✓ 0
  - Paused: ✓ false
  - Pauser: ✓ `5hARLsT1VA2AmuGL2AXUeSyyFG6o2Fcpb9S6aKXNsbeK` (Squads Multisig)
    - Confirmed in forum: https://forum.sky.money/t/atlas-edit-weekly-cycle-proposal-week-of-2025-11-03/27381
  - Unpauser: ✓ `AYPtjx4Hc8us1ikULUedkmZ3wtiD6tmL7gK3qe4V3oHt` (LZ CPI Authority PDA)

### LzReceiveTypes PDA

- Address: `GCzgL229X5dwjSKQADiFMMPUv53RHKujCxXiXbCV6Ert`
- Derivation: ✓ Verified from seeds: `[LzReceiveTypes, OFT Store PDA]`

### OFT Peer Config (EID=30101, Ethereum Mainnet)

- Peer Config PDA: `CwL294rKs4a18rAKDnDs18JsSVoA5Cgz1ekwVPqsQgfR`
- Derivation: ✓ Verified from seeds: `[Peer, OFT Store PDA, eid=30101]`
- Peer Address (hex32): `0x0000000000000000000000001e1d42781fc170ef9da004fb735f56f0276d01b8`
  - Corresponds to: `0x1e1D42781FC170EF9Da004Fb735f56F0276d01B8` (SkyOFTAdapter)

### Enforced Options Configuration

- Send Options:
  - Raw Hex: `00030100110100000000000000000000000000001fbd0`
  - Type: ✓ 3 (Options V3)
  - Kind: ✓ 0x01 (LZ_RECEIVE)
  - Length: ✓ 17 bytes
  - Mode: ✓ 1
  - Value: ✓ 0
  - Gas: ✓ 130,000 compute units
  - Status: ✓ Matches expected configuration
- Send And Call Options: ✓ Same as Send options

### Rate Limiter Configuration

- Outbound Rate Limiter:
  - Capacity: ✓ 10,000,000 USDS
  - Available Capacity: ✓ 9,999,999 USDS (1 USDS was used as test transfer)
  - Refill Per Second: ✓ 115 USDS

  - Rate Limiter Type: ✓ Net
  - Status: ✓ Non-zero (Solana side effectively active as expected)
- Inbound Rate Limiter:
  - Capacity: ✓ 10,000,000 USDS
  - Available Capacity: ✓ 10,000,000 USDS
  - Refill Per Second: ✓ 115 USDS
  - Rate Limiter Type: ✓ Net
  - Status: ✓ Non-zero

#### OFT OApp Registry

- Address: `3JPHRw41T9MX2H6XyZSfrb7Ss8SX3Pa9jgT8Yb5aq4oU`
- Derivation: ✓ Verified from LZ Endpoint seeds: `[OApp, OFT Store PDA]`
- Endpoint Program: `76y77prsiCMvXMjuoZ5VRrhG5qYBrUMYTE5WgHqgjEn6`
- Delegate: ✓ Verified as LZ CPI Authority PDA

### 3.4 Wormhole NTT Program

#### NTT Program

- Program ID: `STTUVCMPuNbk21y1J6nqEGXSQ8HKvFmFBKnCvKHTrWn`
- Status: ✓ Existing program verified

#### NTT Program Data

- Address: `CKKGtQ2m1t4gHUz2tECGQNqaaFtGsoc9eBjzm61qqV2Q`
- Owner: ✓ `BPFLoaderUpgradeab1e11111111111111111111111`
- Upgrade Authority: ✓ `66xDajRZ7MTrgePf27NdugVwDBFhKCCY9EYZ7B9CdDWj` (Wormhole Sky Governance Authority)
- Data Length: ✓ 767,633 bytes

#### NTT Token Authority PDA

- Address: `Bjui9tuxKGsiF5FDwosfUsRUXg9RZCKidbThfm6CRtRt`
- Purpose: Current this is the USDS mint authority (after migration, this will not be the USDS mint authority)

#### NTT Config PDA

- Address: `DCWd3ygRyr9qESyRfPRCMQ6o1wAsPu2niPUc48ixWeY9`
- Derivation: ✓ Verified from seeds: `[config]`
- Owner: ✓ `66xDajRZ7MTrgePf27NdugVwDBFhKCCY9EYZ7B9CdDWj` (Wormhole Sky Governance Authority)

#### New NTT Buffer

- Buffer Address: `43Ggis1nd29QdZFNXQAhhKKj3nxEtwN1DnbNiLf1VfEy`
- Verification: ✓ Matches commit `722c14f4b9cf6073367354bc78bd60fa49b871e6`
- Audited Version: ✓ Same as commit `626962a`
- Authority: ✓ `66xDajRZ7MTrgePf27NdugVwDBFhKCCY9EYZ7B9CdDWj` (Wormhole Sky Governance Authority)
- Data Length: ✓ 758,024 bytes
- Size Check: ✓ New buffer (758,024 bytes) ≤ Existing program (767,633 bytes)
- Purpose: Contains upgraded NTT implementation with:
  - `transfer_burn` function removed

  - Governance-enabled mint authority transfer capability

**Wormhole Governance**

- Wormhole Program: `worm2ZoG2kUd4vFXhvjh93UUH596ayRfgQ2MgjNMTth`
- Wormhole Sky Governance: `SCCGgsntaUPmP6UjwUBNiQQ83ys5fnCHdFASHPV6Fm9`
- Wormhole Sky Governance Authority: `66xDajRZ7MTrgePf27NdugVwDBFhKCCY9EYZ7B9CdDWj`

## 4. Cross-Chain Payload Verification

All payloads were constructed and validated using the `crosschain-gov-solana-spell-payloads` tooling with LiteSVM validation scripts.

In addition the Solana Inspector has been used to simulate each inner instruction: `https://explorer.solana.com/tx/inspector`

The bytecodes were provided by the Keel team at the following commit: `https://github.com/keel-fi/crosschain-gov-solana-spell-payloads/commit/11baa180d4ad6c7579c69c8c0168e17cb73bb6ed`

### 4.1 NTT Transfer Mint Authority Payload

**Configuration Verified:**

- Program ID: ✓ `STTUVCMPuNbk21y1J6nqEGXSQ8HKvFmFBKnCvKHTrWn` (USDS Wormhole NTT)
- Mint: ✓ `USDSwr9ApdHk5bvJKMjzff41FfuX8bSxdKcR81vTwcA` (USDS SPL)
- New Authority: ✓ `BEvTHkTyXooyaJzP8egDUC7WQK8cyRrq5WvERZNWhuah` (USDS OFT Store PDA)
- Governance Program: ✓ `SCCGgsntaUPmP6UjwUBNiQQ83ys5fnCHdFASHPV6Fm9` (Wormhole Governance)
- Current Authority: ✓ `Bjui9tuxKGsiF5FDwosfUsRUXg9RZCKidbThfm6CRtRt` (NTT Token Authority PDA)
- Config PDA Owner: ✓ `66xDajRZ7MTrgePf27NdugVwDBFhKCCY9EYZ7B9CdDWj` (Wormhole Sky Governance Authority)
- Validation: ✓ Payload generated with `wh_owner` sentinel and validate scripts.

**Bytecode (ntt-transfer-mint-authority-mainnet):**

```
000000000000000047656e6572616c507572706f7365476f7665726e616e636502000106742d7ca523a03aaa⌟
↪   fe48abab02e47eb8aef53415cb603c47a3ccf864d86dc006856f43abf4aaa4a26b32ae8ea4cb8fadc8e0⌟
↪   2d267703fbd5f9dad85f6d00b300056f776e657200000000000000000000000000000000000000000000⌟
↪   00000000000100b53f200f8db357f9e1e982ef0ec4b3b879f9f6516d5247307ebaf00d187be51a00009f⌟
↪   92dcb365df21a4a4ec23d8ff4cc020cdd09895f8129c2c2fb43289bc53f95f00000707312d1d41da71f0⌟
↪   fb280c1662cd65ebeb2e0859c0cbae3fdbdcb26c86e0af000106ddf6e1d765a193d9cbe146ceeb79ac1c⌟
↪   b485ed5f5b37913a8cf5857eff00a90000002857edbb54a8aff14b9825dc0cbeaf22836931c00cb89159⌟
↪   2f0a96d0dc6a65a4c67992b01e0db8d122
```

### 4.2 Set Token Freeze Authority Payload

**Configuration Verified**

- Mint: ✓ `USDSwr9ApdHk5bvJKMjzff41FfuX8bSxdKcR81vTwcA` (USDS SPL)
- New Freeze Authority: ✓ `AYPtjx4Hc8us1ikULUedkmZ3wtiD6tmL7gK3qe4V3oHt` (LZ CPI_Authority PDA)
- Current Freeze Authority: ✓ `66xDajRZ7MTrgePf27NdugVwDBFhKCCY9EYZ7B9CdDWj` (Wormhole Sky Governance Authority)
- Governance Program: ✓ Wormhole governance program
- Validation: ✓ Validated via Solana Inspector Simulation and validate scripts.

**Bytecode: (set-token-freeze-authority-mainnet)**

```
000000000000000047656e6572616c507572706f7365476f7665726e616e636502000106742d7ca523a03aaa⌋
↪   fe48abab02e47eb8aef53415cb603c47a3ccf864d86dc006ddf6e1d765a193d9cbe146ceeb79ac1cb485⌋
↪   ed5f5b37913a8cf5857eff00a900020707312d1d41da71f0fb280c1662cd65ebeb2e0859c0cbae3fdbdc⌋
↪   b26c86e0af00016f776e65720000000000000000000000000000000000000000000000000000000010000⌋
↪   230601018dc412529f876c9f3bc01d7c3095bcd6cd1d6d5177b59aa03f04e5c5b422147b
```

### 4.3 Update MPL Metadata Authority Payload

#### Configuration Verified

- Mint: ✓ `USDSwr9ApdHk5bvJKMjzff41FfuX8bSxdKcR81vTwcA` (USDS SPL)
- Metadata PDA Derivation: ✓ Verified from seeds: `[metadata, MPL_PROGRAM, USDS_MINT]`
- New Update Authority: ✓ `AYPtjx4Hc8us1ikULUedkmZ3wtiD6tmL7gK3qe4V3oHt` (LZ CPI_Authority PDA)
- Current Update Authority: ✓ `66xDajRZ7MTrgePf27NdugVwDBFhKCCY9EYZ7B9CdDWj` (Wormhole Sky Governance Authority)
- Validation: ✓ Validated via Solana Inspector Simulation and validate scripts.

**Bytecode: (update-mpl-metadata-authority-mainnet)**

```
000000000000000047656e6572616c507572706f7365476f7665726e616e636502000106742d7ca523a03aaa⌋
↪   fe48abab02e47eb8aef53415cb603c47a3ccf864d86dc00b7065b1e3d17c45389d527f6b04c3cd58b86c⌋
↪   731aa0fdb549b6d1bc03f82946000b6f776e657200000000000000000000000000000000000000000000⌋
↪   000000000001000b7065b1e3d17c45389d527f6b04c3cd58b86c731aa0fdb549b6d1bc03f8294600000b⌋
↪   7065b1e3d17c45389d527f6b04c3cd58b86c731aa0fdb549b6d1bc03f82946000000707312d1d41da71f0⌋
↪   fb280c1662cd65ebeb2e0859c0cbae3fdbdcb26c86e0af000071809dfc828921f70659869a0822bf04c4⌋
↪   2b823d518bfc11fe9a7b65d221a58f00010b7065b1e3d17c45389d527f6b04c3cd58b86c731aa0fdb549⌋
↪   b6d1bc03f82946000070617965720000000000000000000000000000000000000000000000000000001⌋
↪   01000000000000000000000000000000000000000000000000000000000000000000000006a7d517187bd1⌋
↪   6635dad40455fdc2c0c124c68f215675a5dbbacb5f0800000000000b7065b1e3d17c45389d527f6b04c3⌋
↪   cd58b86c731aa0fdb549b6d1bc03f8294600000b7065b1e3d17c45389d527f6b04c3cd58b86c731aa0fd⌋
↪   b549b6d1bc03f829460000002c3201018dc412529f876c9f3bc01d7c3095bcd6cd1d6d5177b59aa03f04⌋
↪   e5c5b422147b000000000000000000
```

### 4.4 Wormhole Program Upgrade Payload

#### Configuration Verified

- NTT Program: ✓ `STTUVCMPuNbk21y1J6nqEGXSQ8HKvFmFBKnCvKHTrWn`
- NTT Program Owner: ✓ `BPFLoaderUpgradeab1e11111111111111111111111`
- NTT ProgramData Owner: ✓ `BPFLoaderUpgradeab1e11111111111111111111111`
- NTT Upgrade Authority: ✓ `66xDajRZ7MTrgePf27NdugVwDBFhKCCY9EYZ7B9CdDWj` (Wormhole Sky Governance Authority)
- New Buffer: ✓ `43Ggis1nd29QdZFNXQAhhKKj3nxEtwN1DnbNiLf1VfEy`
- New Buffer Owner: ✓ `BPFLoaderUpgradeab1e11111111111111111111111`
- New Buffer Authority: ✓ `66xDajRZ7MTrgePf27NdugVwDBFhKCCY9EYZ7B9CdDWj` (Wormhole Sky Governance Authority)
- Spill Account: ✓ KEEL Deployer `PcJcgdWmFZznhhfN28i6T8GHcwA6jmFGuUeNNGvcSY2`
- Validation: ✓ Validated via Solana Inspector Simulation and validate scripts.

**Bytecode: (wh-program-upgrade-mainnet)**

```
0000000000000000047656e6572616c507572706f7365476f7665726e616e636502000106742d7ca523a03aaa┘
↪   fe48abab02e47eb8aef53415cb603c47a3ccf864d86dc002a8f6914e88a1b0e210153ef763ae2b00c2b9┘
↪   3d16c124d2c0537a10048000000007a821ac5164fa9b54fd93b54dba8215550b8fce868f52299169f661┘
↪   9867cac501000106856f43abf4aaa4a26b32ae8ea4cb8fadc8e02d267703fbd5f9dad85f6d00b300012d┘
↪   27f5131975fdaf20a5934c6e90f6d7c9bbde9fcf94c37b48c5a49c7f06aae2000105cab222188023f743┘
↪   94ecaee9daf397c11a2a672511adc34958c1d7bdb1c673000106a7d517192c5c51218cc94c3d4af17f58┘
↪   daee089ba1fd44e3dbd98a00000000000006a7d51718c774c928566398691d5eb68b5eb8a39b4b6d5c73┘
↪   555b210000000000006f776e65720000000000000000000000000000000000000000000000000000001┘
↪   00000403000000
```

### 4.5 Payload Validation Summary

All payloads successfully validated with:

- ✓ No unexpected account modifications
- ✓ Expected lamport transfers only
- ✓ Correct authority derivations
- ✓ Proper governance program usage

## 5. LayerZero Configuration Verification

### 5.1 Governance App DVN Configuration

**Ethereum □ Solana (EID 30168)**

- Block Confirmations: ✓ 15
- DVN Configuration: ✓ 4 of 7 optional DVNs
- DVN List:
  1. LayerZero
  2. Nethermind
  3. Canary
  4. Deutsche Telekom
  5. P2P
  6. Horizon
  7. Luganodes
- Threshold: ✓ 4 signatures required

### 5.2 OFT (Token Bridge) DVN Configuration

**Ethereum □ Solana (EID 30168)**

- Block Confirmations: ✓ 15
- DVN Configuration: ✓ 2 of 2 required DVNs
- DVN List:
  1. LayerZero
  2. Nethermind

**Solana □ Ethereum (EID 30101)**

- Block Confirmations: ✓ 32
- DVN Configuration: ✓ 2 of 2 required DVNs
- DVN List:
  1. LayerZero
  2. Nethermind

## 6 Informational Observations

### Test Transfer Evidence:

- 1 USDS test transfer from Solana to Ethereum was successfully executed
- Evidence visible in Solana OFT outbound rate limiter (9,999,999 available capacity)
- Confirms end-to-end LayerZero bridge functionality

## 7. Verification Methodology

Our verification process employed a multi-layered approach:

1. **Source Code Review**
   - Verified all repository commit hashes
   - Confirmed code matches audited versions
   - Reviewed all changes since audit
2. **Bytecode Verification**
   - Used `forge verify-bytecode` for EVM contracts
   - Used `solana-verify` for Solana programs
   - Validated compiler settings (viaIR, evm_version, etc.)
3. **On-Chain State Verification**
   - Queried live mainnet state via RPC
   - Parsed and decoded binary account data
   - Validated all configuration parameters
4. **Cross-Chain Mapping Verification**
   - Verified bidirectional peer relationships
   - Validated address format conversions (EVM ▯ Solana)
   - Confirmed EID configurations
5. **PDA Derivation Verification**
   - Independently derived all PDAs from seeds
   - Validated bump seeds
   - Verified PDA ownership and program associations
6. **Payload Construction and Validation**
   - Used official payload tooling
   - Validated with existing validate scripts and Solana Transaction Inspector simulations
   - Confirmed no unexpected state changes
7. **Script-Based Automation**
   - Developed comprehensive verification scripts
   - Automated binary parsing and decoding
   - Created reproducible verification procedures

## 8. Conclusion

Our verification confirms that:

1. ✓ All deployed contracts and programs match audited source code
2. ✓ All cross-chain configurations are correctly established
3. ✓ All access controls are properly configured
4. ✓ All PDAs are correctly derived and verified
5. ✓ All payloads are correctly constructed and validated
6. ✓ All rate limiters are properly configured
7. ✓ All DVN configurations provide adequate security
8. ✓ The migration plan follows a safe, atomic approach
9. ✓ All pre-migration state is as expected
10. ✓ End-to-end bridge functionality has been demonstrated

The USDS bridge migration from Wormhole to LayerZero is ready to proceed with the two-spell execution plan.

All technical components have been verified for correctness according to thee migration design.

**Key Addresses and Accounts Reference**

**Ethereum Mainnet:**

- USDS: `0xdc035d45d973e3ec169d2276ddab16f1e407384f`
- MCD_PAUSE_PROXY: `0xbe8e3e3618f7474f8cb1d074a26affef007e98fb`
- L1GovernanceRelay: `0x2beBFe397D497b66cB14461cB6ee467b4C3B7D61`
- GovernanceOAppSender: `0x27FC1DD771817b53bE48Dc28789533BEa53C9CCA`
- SkyOFTAdapter: `0x1e1D42781FC170EF9da004Fb735f56F0276d01B8`
- NTT Manager Proxy: `0x7d4958454a3f520bDA8be764d06591B054B0bf33`
- New NTT Manager Impl: `0xD4DD90bAC23E2a1470681E7cAfFD381FE44c3430`

**Solana Mainnet:**

- USDS Mint: `USDSwr9ApdHk5bvJKMjzff41FfuX8bSxdKcR81vTwcA`
- LZ Governance Program: `SKYGRikJcGSa3jC5HDyzDrVsmkCk3e5SqAurycny8PW`
- LZ Gov PDA: `8vXXGiaXFrKFUDw21H5Z57ex552Lh8WP9rVd2ktzmcCy`
- LZ CPI Authority PDA: `AYPtjx4Hc8us1ikULUedkmZ3wtiD6tmL7gK3qe4V3oHt`
- Sky OFT Program: `SKYTAiJRkgexqQqFoqhXdCANyfziwrVrzjhBaCzdbKW`
- OFT Store PDA: `BEvTHkTyXooyaJzP8egDUC7WQK8cyRrq5WvERZNWhuah`
- NTT Program: `STTUVCMPuNbk21y1J6nqEGXSQ8HKvFmFBKnCvKHTrWn`
- NTT Token Authority PDA: `Bjui9tuxKGsiF5FDwosfUsRUXg9RZCKidbThfm6CRtRt`
- New NTT Buffer: `43Ggis1nd29QdZFNXQAhhKKj3nxEtwN1DnbNiLf1VfEy`
- Wormhole Sky Governance Authority: `66xDajRZ7MTrgePf27NdugVwDBFhKCCY9EYZ7B9CdDWj`

# 3 Findings

## 3.1 Medium Risk

### 3.1.1 Incorrect `newMintAuthority` in the payload to migrate the USDS mint authority on Solana from NTT to OFT

**Severity:** Medium Risk

**Context:** ntt-transfer-mint-authority-mainnet.txt

**Description:** The USDS token on Solana has a mint authority account held by an NTT program PDA.

As part of the migration process to the LayerZero OFT infrastructure, the `mintAuthority` needs to be transferred to `BEvTHkTyXooyaJzP8egDUC7WQK8cyRrq5WvERZNWhuah` (OFT Mint Authority / OFT Store PDA).

Scripts are used to generate the payload for the NTT mint ownership transfer on Solana. These payloads are used in the Sky governance process on Ethereum (spells). The Sky spell execution on Ethereum triggers a Wormhole bridge transactions that use the payload to execute the ownership transfer on Solana.

However, in the reviewed version, the payload included an incorrect `newMintAuthority`.
The `newMintAuthority` should be `BEvTHkTyXooyaJzP8egDUC7WQK8cyRrq5WvERZNWhuah` (OFT Mint Authority / OFT Store), not `AYPtjx4Hc8us1ikULUedkmZ3wtiD6tmL7gK3qe4V3oHt` (SKY_LZ_GOVERNANCE_CPI_AUTHORITY).

This error would prevent the new OFT from functioning correctly, as it would no longer be possible to mint new USDS on Solana after users lock USDS on the OFT contract on Ethereum.

The `SKY_LZ_GOVERNANCE_CPI_AUTHORITY` is a PDA controlled by Sky governance, so it would still be possible to recover by transferring the mint authority to the correct account through a follow-up governance action.

We believe this happened because of an incorrect comment at PR 18.

**Recommendation:** Update the `newMintAuthority` in the config to `BEvTHkTyXooyaJzP8egDUC7WQK8cyRrq5WvERZNWhuah` (OFT Mint Authority). Afterwards, regenerate and validate the payload.

**Sky:** Fixed in commit 11baa18.

**Cantina Managed:** Fixed.

## 3.2 Low Risk

### 3.2.1 Migration test run on Solana `devnet` upgraded the `NTTManager` to an incorrect older version

**Severity:** Low Risk

**Context:** transfer_mint_authority.rs#L41

**Description:** As part of the bridge migration for USDS from Wormhole NTT to LayerZero OFT, it is required to upgrade the NTTManager on Solana to transfer the mint authority to the OFT.

To ensure correctness, an end-to-end test was performed on Solana `devnet`, where the NTTManager was upgraded via a bridge transaction from Ethereum.

However, after inspecting the new version of the NTTManager, an incorrect NTT Program version was identified.

After the upgrade, the `transfer_mint_authority` corresponded to NTT Program version: 832781e

Which still included an older owner check

```
assert!(ctx.accounts.config.owner == ctx.accounts.payer.key(), "Only the owner can
↪  transfer the mint authority");
```

The recommend check in the correct version instead of using `assert` is:

```rust
pub owner: Signer<'info>,
#[account(
    has_one = owner,
)]
pub config: Account<'info, Config>
```

The correct NTT Program version to be used on mainnet is: 722c14f

**Recommendation:** Use the same version for the test-run on devnet as on Mainnet.

**Sky:** A devnet test-run has been performed with the correct version and the results were shared with the reviewers.

**Cantina Managed:** Fixed.