CANTINA

Sky OFT: Cross-chain Governance Payloads

Security Review

Cantina Managed review by:
Christoph Michel, Lead Security Researcher
M4rio.eth, Lead Security Researcher

May 4, 2026

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.

On May 4th the Cantina team conducted a review of sky-oapp-oft on commit hash 055886ca.

2.1 Scope

The security review focused on sky-oapp-oft on commit hash 055886ca along with the three Solana governance payloads (Unpause OFT, Set Inbound Rate Limit, Set Outbound Rate Limit) targeting the Sky OFT on Solana mainnet.

2.2 Codebase context

The reviewed commit adds payload-generation and simulation tooling for Solana governance messages targeting the Sky OFT on Solana mainnet. The generated payloads consist of the `dstTarget` and `dstCallData` values that an Ethereum Maker/Sky executive spell is expected to pass to the L1 Governance Relay / LayerZero governance OApp for delivery to Solana.

Three governance actions are covered by the tooling:

1. Unpausing the Sky OFT on Solana.
2. Setting the Ethereum-to-Solana inbound rate limit on the Sky OFT.
3. Setting the Solana-to-Ethereum outbound rate limit on the Sky OFT.

For each action, the tooling produces the `dstTarget` (the OFT program ID encoded as `bytes32`) and the `dstCallData` (the body of the `GovernanceMessage`, comprising the accounts list and the Solana instruction data consumed by the Sky governance program on Solana). Together, these are the two values needed by `GovernanceOAppSender::TxParams` on L1.

The relevant Solana mainnet accounts referenced by the payloads are:

- OFT program: `SKYTAiJRkgexqQqFoqhXdCANyfziwrVrzjhBaCzdbKW`
- OFT store: `BEvTHkTyXooyaJzP8egDUC7WQK8cyRrq5WvERZNWhuah`
- L1 Gov Relay CPI authority on Solana: `AYPtjx4Hc8us1ikULUedkmZ3wtiD6tmL7gK3qe4V3oHt`
- Ethereum peer config PDA: `CwL294rKs4a18rAKDnDs18JsSVoA5Cgz1ekwVPqsQgfR`

2.3 Cantina Managed Team Statement

The Cantina Managed team reviewed `sky-ecosystem/sky-oapp-oft` at commit `1a9b2fbc54dd848b62ef115adc282d7d9f537175`. The reviewed commit adds payload-generation and simulation tooling for Solana governance messages targeting the Sky OFT on Solana mainnet. The generated payloads consist of the `dstTarget` and `dstCallData` values that an Ethereum Maker/Sky executive spell is expected to pass to the L1 Governance Relay / LayerZero governance OApp for delivery to Solana.

We verified that the reviewed payload bytes decode to the intended Solana OFT instructions and replay successfully in Solana mainnet simulation, confirming the expected effects:

- unpausing the OFT,
- updating the Ethereum-to-Solana inbound rate limit, and
- updating the Solana-to-Ethereum outbound rate limit.

The Solana side requires the `cpi_authority` PDA corresponding to the EVM L1GovernanceRelay, because the OFT admin/unpauser is set to that derived PDA. This means the LayerZero message must be initiated through the `L1GovernanceRelay` = `0x2beBFe397D497b66cB14461cB6ee467b4C3B7D61` contract. Currently, `GovernanceOAppSender.canCallTarget(L1GovernanceRelay, 30168, OFT_PROGRAM_BYTES32) == false`.
It must be set to true by the `GovernanceOAppSender` owner before the

`L1GovernanceRelay.relayRaw(...)` payloads can be dispatched, via `setCanCallTarget(L1GovernanceRelay, 30168, OFT_PROGRAM_BYTES32, true)` with

- `L1GovernanceRelay` = `0x2beBFe397D497b66cB14461cB6ee467b4C3B7D61`
- `OFT_PROGRAM_BYTES32` = `0x067c7c6c60ba7f1aec14059100df74d6da07e7d31da5dd756c6308f02e661649` (`SKYTAiJRkgexqQqFoqhXdCANyfziwrVrzjhBaCzdbKW`)

2.3.1 Verification command

The following command was used to verify that the generated `dstTarget` and `dstCallData` values match the reviewed payloads for all three actions, after updating the rate-limit test parameters to the intended production values (`refill_per_second = 57,870,370` and `capacity = 5,000,000,000,000`):

```
OFT_ID=SKYTAiJRkgexqQqFoqhXdCANyfziwrVrzjhBaCzdbKW \
GOVERNANCE_ID=SKYGRikJcGSa3jC5HDyzDrVsmkCk3e5SqAurycny8PW \
cargo test -p governance --test msg_codec -- --show-output \
  test_governance_message_unpause_oft \
  test_set_inbound_rate_limit \
  test_set_outbound_rate_limit
```

2.3.2 Reviewed payloads

1. Unpause Sky OFT **Effect:** sets `OFTStore.paused = false` on the Solana Sky OFT.

dstTarget:

```
0x067c7c6c60ba7f1aec14059100df74d6da07e7d31da5dd756c6308f02e661649
```

dstCallData:

```
0x00026370695f617574686f726974790000000000000000000000000000000000000001009825dc0cbeaf22
↪  836931c00cb891592f0a96d0dc6a65a4c67992b01e0db8d12200013f209a0238674f2d00
```

2. Set inbound rate limit (Ethereum → Solana) **Effect:** updates the Ethereum peer inbound rate limiter on the Solana Sky OFT.

Values:

- `refill_per_second = 57,870,370`
- `capacity = 5,000,000,000,000`
- `rate_limiter_type = Net`

dstTarget:

```
0x067c7c6c60ba7f1aec14059100df74d6da07e7d31da5dd756c6308f02e661649
```

dstCallData:

```
0x00046370695f617574686f726974790000000000000000000000000000000000000101b15b6cea974229
↪  517bec70478d3f574b4010444df812d75f6ca722fc0fa3256800019825dc0cbeaf22836931c00cb89159
↪  2f0a96d0dc6a65a4c67992b01e0db8d1220000000000000000000000000000000000000000000000000
↪  00000000000000000000004fbba8398b8c5d2f9575000004010122087303000000000001005039278c0400
↪  000100
```

3. Set outbound rate limit (Solana → Ethereum) **Effect:** updates the Ethereum peer outbound rate limiter on the Solana Sky OFT.

Values:

- `refill_per_second = 57,870,370`
- `capacity = 5,000,000,000,000`
- `rate_limiter_type = Net`

dstTarget:

```
0x067c7c6c60ba7f1aec14059100df74d6da07e7d31da5dd756c6308f02e661649
```

dstCallData:

```
0x00046370695f617574686f726974790000000000000000000000000000000101b15b6cea974229
↪ 517bec70478d3f574b4010444df812d75f6ca722fc0fa3256800019825dc0cbeaf22836931c00cb89159
↪ 2f0a96d0dc6a65a4c67992b01e0db8d1220000000000000000000000000000000000000000000000000
↪ 0000000000000000000004fbba8398b8c5d2f9575000030101220873030000000001005039278c0400
↪ 000100
```

2.3.3 Executor options

LayerZero receive options.

Proposed `extraOptions` for all three sends: `0x0003010011010000000000000000000000000927c0`. Decoded:

Field	Value
Options type	`0x0003` (`TYPE_3`)
Worker id	`0x01` (LayerZero executor)
Executor option length	`0x0011` = 17 bytes
Executor option type	`0x01` (`LZ_RECEIVE`)
lzReceive gas	`600_000` destination execution gas / Solana compute budget
lzReceive value	0

The proposed 600,000 CU is reasonable and leaves a lot of room over the estimated ∼150,000 CU upper-bound from the referenced end-to-end Solana LayerZero test transaction and the additional inner target instruction cost.

`GovernanceOAppSender.enforcedOptions(dstEid, SEND_TX)` on Ethereum was also checked. No enforced options are configured for Solana (`dstEid` = 30168). Therefore the executor options are not supplied by protocol-level enforced options and must indeed be fully defined via the custom `extraOptions` in each send.

3 Appendix

3.1 Sky OFT — Cross-Chain Governance Payloads (Solana mainnet)

Three governance payloads to be forwarded by the L1 Gov Relay (Ethereum) to the Sky OFT on Solana mainnet:

1. Unpause the OFT
2. Set inbound rate limit (Ethereum → Solana)
3. Set outbound rate limit (Solana → Ethereum)

For each payload, `dstTarget` is the OFT program ID encoded as `bytes32`. `dstCallData` is the body of the `GovernanceMessage` (accounts list + Solana instruction data) consumed by the Sky governance program on Solana. They are the two values needed by `GovernanceOAppSender::TxParams` on L1.

Reference accounts on Solana mainnet:

- OFT program: `SKYTAiJRkgexqQqFoqhXdCANyfziwrVrzjhBaCzdbKW`
- OFT store: `BEvTHkTyXooyaJzP8egDUC7WQK8cyRrq5WvERZNWhuah`
- L1 Gov Relay CPI authority on Solana: `AYPtjx4Hc8us1ikULUedkmZ3wtiD6tmL7gK3qe4V3oHt`
- Ethereum peer config PDA: `CwL294rKs4a18rAKDnDs18JsSVoA5Cgz1ekwVPqsQgfR`

3.1.1 1. Unpause OFT

Effect: sets `OFTStore.paused = false` on the Sky OFT, executed under the L1 Gov Relay CPI authority.

```
dstTarget:   0x067c7c6c60ba7f1aec14059100df74d6da07e7d31da5dd756c6308f02e661649
dstCallData: 0x00026370695f617574686f72697479000000000000000000000000000000000000000001009
↪   825dc0cbeaf22836931c00cb891592f0a96d0dc6a65a4c67992b01e0db8d12200013f209a0238674f2d00
```

Solana simulation message (base64) for Method B validation:


```
AgEBBPfyQalUpvd/yPKWTVNJRDz4284JN7je+m+J1vwpwGm7jcQSUp+HbJ87wB18MJW81s0dbVF3tZqgPwTlxbQi
↪   FHuYJdwMvq8ig2kxwAy4kVkvCpbQ3GplpMZ5krAeDbjRIgZ8fGxgun8a7BQFkQDfdNbaB+fTHaXddWxjCPAu
↪   ZhZJAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABAwIBAgk/IJoCOGdPLQA=
```


3.1.2 2. Set Inbound Rate Limit (Ethereum → Solana)

Effect: sets the Ethereum-mainnet peer's inbound rate limiter on the Sky OFT to:

- `refill_per_second: 57_870_370`
- `capacity:          5_000_000_000_000`
- `rate_limiter_type: Net`

Executed under the L1 Gov Relay CPI authority.

```
dstTarget:   0x067c7c6c60ba7f1aec14059100df74d6da07e7d31da5dd756c6308f02e661649
dstCallData: 0x00046370695f617574686f7269747900000000000000000000000000000000000000000101b
↪   15b6cea974229517bec70478d3f574b4010444df812d75f6ca722fc0fa3256800019825dc0cbeaf22836
↪   931c00cb891592f0a96d0dc6a65a4c67992b01e0db8d1220000000000000000000000000000000000000
↪   0000000000000000000000000000000000004fbba8398b8c5d2f957500004010122087303000000000010
↪   05039278c0400000100
```

Solana simulation message (base64) for Method B validation:


```
AgADBvfyQalUpvd/yPKWTVNJRDz4284JN7je+m+J1vwpwGm7jcQSUp+HbJ87wB18MJW81s0dbVF3tZqgPwTlxbQi
↪   FHuxW2zql0IpUXvscEeNP1dLQBBETfgS119spyL8D6MlaAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
↪   AAAABnx8bGC6fxrsFAWRAN901toH59Mdpd11bGMI8C5mFkmYJdwMvq8ig2kxwAy4kVkvCpbQ3GplpMZ5krAe
↪   DbjRIgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQQEAQIFAyJPu6g5i4xdL5V1AAAEAQEiCHMD
↪   AAAAAAEAUDknjAQAAAEA
```

3.1.3 3. Set Outbound Rate Limit (Solana → Ethereum)

Effect: sets the Ethereum-mainnet peer's outbound rate limiter on the Sky OFT to:

- `refill_per_second: 57_870_370`
- `capacity:          5_000_000_000_000`
- `rate_limiter_type: Net`

Executed under the L1 Gov Relay CPI authority.

```
dstTarget:   0x067c7c6c60ba7f1aec14059100df74d6da07e7d31da5dd756c6308f02e661649
dstCallData: 0x00046370695f617574686f726974790000000000000000000000000000000000000000101b
    15b6cea974229517bec70478d3f574b4010444df812d75f6ca722fc0fa3256800019825dc0cbeaf22836
    931c00cb891592f0a96d0dc6a65a4c67992b01e0db8d1220000000000000000000000000000000000000
    0000000000000000000000000000000000004fbba8398b8c5d2f95750000301012208730300000000010
    05039278c0400000100
```

Solana simulation message (base64) for Method B validation:


```
AgADBvfyQalUpvd/yPKWTVNJRDz4284JN7je+m+J1vwpwGm7jcQSUp+HbJ87wB18MJW81s0dbVF3tZqgPwTlxbQi
    FHuxW2zql0IpUXvscEeNP1dLQBBETfgS119spyL8D6MlaAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
    AAAABnx8bGC6fxrsFAWRAN901toH59Mdpd11bGMI8C5mFkmYJdwMvq8ig2kxwAy4kVkvCpbQ3GplpMZ5krAe
    DbjRIgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQQEAQIFAyJPu6g5i4xdL5V1AAADAQEiCHMD
    AAAAAAEAUDknjAQAAAEA
```