Solana SPL Token Whitelist Audit Report

Prepared by Cyfrin

Version 2.0

Lead Auditors

DadeKuma

Naman

October 31, 2025

Contents

1 About Cyfrin 2

2 Disclaimer 2

3 Risk Classification 2

4 Protocol Summary 2

5 Audit Scope 2

6 Executive Summary 3

7 Findings 4

7.1 Informational 4

7.1.1 Permanent delegate extension creates irreversible token control risk 4

1 About Cyfrin

Cyfrin is a Web3 security company dedicated to bringing industry-leading protection and education to our partners and their projects. Our goal is to create a safe, reliable, and transparent environment for everyone in Web3 and DeFi. Learn more about us at cyfrin.io.

2 Disclaimer

The Cyfrin team makes every effort to find as many vulnerabilities in the code as possible in the given time but holds no responsibility for the findings in this document. A security audit by the team does not endorse the underlying business or product. The audit was time-boxed and the review of the code was solely on the security aspects of the solidity implementation of the contracts.

3 Risk Classification

	Impact: High	**Impact: Medium**	**Impact: Low**
Likelihood: High	Critical	High	Medium
Likelihood: Medium	High	Medium	Low
Likelihood: Low	Medium	Low	Low

4 Protocol Summary

The SPL Token Whitelist manages the technical token access control by handling the unfreezing of SPL Token-2022 accounts. Token accounts are initially created in a frozen state, preventing transfers until investors complete the whitelisting process.

Upon successful whitelisting, this program validates account ownership, mint association, and frozen status before executing batch thaw operations using the mint's freeze authority. The program accepts multiple token accounts in a single transaction through the remaining_accounts pattern, enabling efficient whitelisting of investors with multiple token positions.

The program uses common administrative framework featuring role-based access control with a single admin authority, atomic admin transfer capabilities with duplicate-prevention checks, and synchronized pause/unpause mechanisms. The architecture prioritizes operational flexibility and emergency response capabilities while maintaining strict separation of concerns between identity verification and token custody layers.

5 Audit Scope

The audit scope was limited to:

```
programs/spl-token-whitelist/src/instructions/admin/change_admin.rs
programs/spl-token-whitelist/src/instructions/admin/initialize.rs
programs/spl-token-whitelist/src/instructions/admin/mod.rs
programs/spl-token-whitelist/src/instructions/admin/pause.rs
programs/spl-token-whitelist/src/instructions/admin/unpause.rs
programs/spl-token-whitelist/src/instructions/mod.rs
programs/spl-token-whitelist/src/instructions/whitelist.rs
programs/spl-token-whitelist/src/states/mod.rs
programs/spl-token-whitelist/src/states/spl_whitelist_state.rs
programs/spl-token-whitelist/src/constants.rs
programs/spl-token-whitelist/src/errors.rs
programs/spl-token-whitelist/src/events.rs
```

```
programs/spl-token-whitelist/src/lib.rs
```

6 Executive Summary

Over the course of 2 days, the Cyfrin team conducted an audit on the Solana SPL Token Whitelist smart contracts provided by Securitize. In this period, a total of 1 issues were found.

Summary

Project Name	Solana SPL Token Whitelist
Repository	bc-solana-whitelist-sc
Commit	053338c40467...
Audit Timeline	Oct 30th - Oct 31st, 2025
Methods	Manual Review

Issues Found

Critical Risk	0
High Risk	0
Medium Risk	0
Low Risk	0
Informational	1
Gas Optimizations	0
Total Issues	1

Summary of Findings

[I-1] Permanent delegate extension creates irreversible token control risk	Acknowledged

7 Findings

7.1 Informational

7.1.1 Permanent delegate extension creates irreversible token control risk

Description: The SPL whitelisting module supports mints with the permanent delegate extension, which grants irrevocable token control authority that bypasses standard token account ownership.

Impact: Once established, the permanent delegate authority cannot be revoked or modified.

Unlike standard delegates that token owners can remove, this permanent delegate maintains perpetual authority to transfer, burn, and freeze tokens across all accounts of that mint, creating an irreversible centralization risk.

Proof of Concept: Tests confirm that mints are initialized with the `PermanentDelegate` extension enabled, granting permanent control to the designated delegate.

Recommended Mitigation: Consider removing the permanent delegate extension unless absolutely required for external processes. If it is necessary, consider clearly documenting this risk, so users understand the immutable control implications.

Securitize: Acknowledged.