Cyberscope

A TAC Security Company

Formal Statement

Fair

December 2025

Programs:

EGxd8LCM8Y1uMyXrWWapEMh9tH2whZaNBYhaV29Mq9fb

T1ACXXh9Xp15oKrh3s9REJnUtrUqbJ4xFEq2fege8Wv

Audited by © cyberscope

Table of Contents

Risk Classification

The criticality of findings in Cyberscope’s smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

Severity	Likelihood / Impact of Exploitation
● Critical	Highly Likely / High Impact
● Medium	Less Likely / High Impact or Highly Likely/ Lower Impact
● Minor / Informative	Unlikely / Low to no Impact

Review

Audit Updates

Programs	EGxd8LCM8Y1uMyXrWWapEMh9tH2whZaNBYhaV29Mq9fb T1ACXXh9Xp15oKrh3s9REJnUtrUqbJ4xFEq2fege8Wv

Source Files

Filename	SHA256
lib.rs	a628e12427066634e24db6e8f4de4054138efd4f740f2c386218c88a21c156b9

Formal Statement

As of the current on-chain state and corroborating our November 2025 audit conducted by Cyberscope:

- **Program Integrity:** The deployed program at address `EGxd8LCM8Y1uMyXrWWapEMh9tH2whZaNBYhaV29Mq9fb` has been verified against the audited source code through a reproducible build process, confirming byte-for-byte consistency with the code reviewed during the audit.

- **Token Control:** The TIAC token, with mint address `T1ACXXh9Xp15oKrh3s9REJnUtrUqbJ4xFEq2fege8Wv`, is governed by the FAIR program, whose deployment and logic were reviewed and audited in November 2025. The mint authority for this token is controlled exclusively by the program-derived address (PDA) established by the FAIR program, ensuring trustless operation according to the audited design.

- **Upgrade Authority:** The program's upgrade authority has been permanently renounced, guaranteeing that no further modifications to the program code can be made. This preserves the integrity of the audited program logic and enforces immutability.

- **Security Properties & Program Invariants:**

  `MIN_SUPPLY_TOKENS` is set to 100,000 TIAC, ensuring that the initial sale and subsequent token operations enforce a hard minimum supply.

  The `sale_end` parameter is set to January 31, 2026, 23:59 UTC, establishing the defined closure of the initial sale period as enforced by the program logic.

These confirmations demonstrate that the TIAC token operates under the guarantees and security properties defined in the **FAIR program audit**, with the program logic immutable, mint authority secured under the program PDA, and initial sale parameters accurately reflected on-chain.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope’s prior written consent. This report is not nor should be considered an “endorsement” or “disapproval” of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any “product” or “asset” created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope’s position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a TAC blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

A *TAC Security* Company

The Cyberscope team

cyberscope.io