This document is intended as a response to the Gero team (POC: Chris Chiras) from MLabs (POC: Ben Hart) regarding the points of the audit report of the Gero onchain-governance module supplied by Tweag. We discuss each item and provide our professional opinions as the core developers of the smart-contracts in question.

Audit Item Index	**Response and Justification**
2.2.1.1 – User tokens can be stolen by public keys	This vulnerability was marked as critical by Tweag and promptly resolved on the MLabs side by a later commit. Per Tweag's policy as an auditor, they could not provide professional feedback on the resolution; however, MLabs has integrated the test cases provided by Tweag to verify that the vulnerability was indeed resolved.
2.2.4.1 – Unclear role of the Gov validator and token	While this was marked by Tweag as high-severity, we at MLabs are confused as to why it was categorized as any sort of vulnerability; the role of the Gov validator, while redundant and believed by us to indeed be dead code, does not cause any errors, and the contract as-is fixes all known issues. Moreover, while we can speculate about unknown exploits that could emerge as a result of this issue, none have been found, and we risk a new set of exploits that would occur as a result of implementing the fix; this would require another round of audit from Tweag, and since the auditors missed this once in the first audit, there's no telling if they might miss another similar issue.
2.2.1.2 – The minting policy of the Gov token mostly relies on trusting the administrator	As per the specification, this protocol cannot remove trust from the admin, and as such, the model is built around this. By providing analysis tools to the user, and always allowing them to exit the protocol, the user accepts that the administrator is ultimately always in a position of power. This issue is by design. Note however, the Admin never has the ability to steal funds or rewards from the user via the protocol.
2.2.3.1 – Error reporting is lacking	Error reporting will be handled by the offchain, by writing it such that it would never submit a failing transaction. Some errors have been removed from on-chain to save on script size.

2.2.2.1 – User ids are not reused	Significant logic would be required to enable this, and given the maximum id is 256^29, this is a non-issue.
2.2.2.2 – No specification on burning Gov tokens	The contract is not expected to close directly through its original policy for simplicity. If cleanup is desired, the tokens could be sent to a neverspend script.
2.2.2.3 – Unclear meaning of zero votes	This has been fixed, zero vote positions are now impossible.
2.2.2.4 – gsPolicyIds is an unused and immutable piece of datum	The gsPolicyIds field is meant as a declaration of reward policies on-chain and exists solely for record keeping.
2.2.3.2 – Dead code	Remaining utility functions from a previous version, these have been removed.
2.2.3.3 – Undocumented code section regarding closing positions	Comments have been added to this section, documentation updated.
2.2.2.5 – Specification mentions unimplemented features	These are offchain features, unimplemented at time of audit, which was on-chain only.
2.2.2.6 – Various minor concerns with the specification	All concerns addressed.
2.2.3.4 – Various minor code quality concerns	All concerns addressed.