Trail of Bits SNS Re-Review: Fix Notes

The issues in the report were addressed as follows.

Issue	Severity	Status
TOB-DFSNSR-1	Low	Resolved
TOB-DFSNSR-3	Medium	Resolved
TOB-DFSNSR-4	Informational	Resolved
TOB-DFSNSR-5	Informational	Resolved

TOB-DFSNSR-1: Uneven distribution of stake across neurons may impact SNS governance

Status: Resolved

Commit: https://github.com/dfinity/ic/commit/846ec5b8521af25cab39942448d4ba2f9e5b4407

Comment: Took their recommendation: more evenly apportion SNS tokens such that the difference is at most 1 e8s.

TOB-DFSNSR-3: Wrong error message returned from new_sale_ticket in Adopted state

Status: Resolved

Commit: https://github.com/dfinity/ic/commit/71777add0af30e8152880d462fe9d292fbdf4cdd

Comment: Replaced use of > and < operators with calls to a couple of new methods: is_after_open is_before_open.

TOB-DFSNSR-4: Swap canister paging implementations panic on invalid ranges

Status: Resolved

Commit: https://github.com/dfinity/ic/commit/0a92176c85d7a4da2b9789a01fa29d49284969a7

Comment: Added code to specially handle when a large offset is passed.

TOB-DFSNSR-5: The NNS governance canister always warns about missing neurons if a token swap fails

Status: Resolved

Commit: https://github.com/dfinity/ic/commit/3c15ba563eedf8b70086e5ed7e17e1b20e1955dc

Comment: Added guard around logging statement so that logging only occurs when missing_neurons is nonempty.

Quality Recommendations (Appendix D)

- Update the comment for the sale neuron memo range
  - The review suggested that the upper bound for neuron memos has not been enforced, but in fact it has been (via the sns-init crate). Still, to make the code clearer, we renamed `SALE_NEURON_MEMO_RANGE` to `NEURON_BASKET_MEMO_RANGE` and updated the comment.
  - https://github.com/dfinity/ic/commit/2c6298eb5fbb1c144c3a5b5405bd02f8b4e7a761
- Update the unit used in the log message
  - Addressed by using the `Duration` crate for producing human-readable time units in logs.
  - https://github.com/dfinity/ic/commit/49f09f95484f71058242f74f0bf11892e68ddc26
- Update the comment for `FIRST_PRINCIPAL_BYTES`
  - Corrected and expanded the doc comment.
  - https://github.com/dfinity/ic/commit/d6d3c37862698db8f553a4da473f5e090e754e8a
- Update the comment for `Swap::can_open`
  - The NNS team agreed that the code and the comments are technically correct, but we simplified the code, improving readability and removing extraneous checks in Swap heartbeat.
  - https://github.com/dfinity/ic/commit/4eabd5794af5c81347ceb5e16aff71ed1d03bf23
- Remove the `ValidGovernanceProto::validate_canister_id_field` method
  - Since there is no immediate risk, DFINITY has factored this out into a separate ticket for future prioritization.
- Avoid using `as` when casting from larger to smaller integer types
  - Opt for u64 arithmetic rather than `usize` arithmetic.
  - https://github.com/dfinity/ic/commit/eb8788424e7ec13556269a69ffff22f454062e8f