Security Council Elections

Update: Tally vote : [Tally | Arbitrum Proposal](#)

Category: Constitutional - Process

As part of its governance, the Arbitrum DAO incorporates a Security Council that can take certain emergency and non-emergency actions:

- [Section 3 of the Constitution](#) describes this council in more detail.

- [Initial Setup Transparency Report](#) details the current members of the council.

- [Section 4 on the Constitution](#) outlines an election process that will replace six security council members every six months.

The first election to replace the first cohort of Security Council Members is expected to begin on the 15th September.

Executive summary

- This vote relates to the enactment of the Arbitrum Security Council elections.

- A smart contract system has been developed to enable on-chain voting. That system is final and has undergone multiple security audits.

- This vote is meant to enable the smart contract system that will allow for the elections, as well as temperature check with the DAO.

- A successful vote will lead to an on-chain proposal that updates the constitution text with the new sections below, as well as the new Security Council election system being activated within the broader [Arbitrum governance architecture](#).

Implementation Status

The code representing the proposed architecture is final and available for full review in:

[Merge pull request #181 from ArbitrumFoundation/scm-deploy-gnosis-saf… · ArbitrumFoundation/governance@46dd56f · GitHub](#).

The work has already been audited by Trail of Bits and the identified issues have been patched, the full audit report is available [here](#).

A Code4Rena audit competition has also been completed for the election system.

Background

An overview of the election process as described by the Constitution

alongside the process for how to enact a code change to Arbitrum's smart

contract suite:

Comment

- [Constitution of the Arbitrum DAO](#) (esp. sections [3](#) and [4](#)) - As noted above, this proposal seeks to enact what is already described in the Constitution.

- [DAO Governance Architecture](#) - The proposed architecture makes use of a number of existing governance components.

An understanding of the following smart contract suites will help the

reader evaluate this proposal as it re-uses several components:

- [Open Zeppelin Governor](#) - The proposed architecture inherits a number of OpenZeppelin contracts.

- [Gnosis Modules](#) - Each of the security councils is a Gnosis Safe, and updating members of the security council is handled via adding Gnosis modules.

High-level Election Overview

The Constitution specifies that membership of the Security Council is split into two cohorts. Every 6 months, all positions in a single cohort are put up for election.

The proposed election implementation, which must adhere to [the specification laid out in the Constitution](#) is split into:

- Election stages: The process for selecting and voting for nominees.

- Update stages: Installing the newly elected cohort into the Arbitrum smart contracts.

The election process and update stages are performed via on-chain smart contracts. A brief overview of each stage includes:

Election Stages

Process for selecting and voting for the new cohort of Security council members.

1. Nominee selection (7 days). Candidates must gain 0.2% of total votable tokens in order to make it to the next step.

2. Compliance check by Foundation (14 days). As dictated in the Constitution, the selected nominees must undergo a compliance check to ensure they comply with the legal requirements, service agreements, and additional rules dictated by the Constitution.

3. Member election (21 days). Votes are cast and the top 6 nominees are selected.

Update Stages

Process to install the newly elected cohort of Security Council members into the Arbitrum smart contracts.

1. Security Council manager update (0 days). The manager is the source of truth for specifying who are the current council members. It processes the election result and takes note on who will be the new security council members.

2. L2 timelock + withdrawal + L1 timelock (3 + 7 + 3 days). All actions that directly affect the core Arbitrum contracts must go through a series of timelocks to protect the right for all users to exit. This is a built-in safety mechanism for users who are unhappy with the approved changes.

3. Individual council update (0 days). Once the updates have passed through the relevant timelocks, the Security Council manager can install the security council members. This requires updating 4 Gnosis Safe smart contracts that are controlled by the Security Council members.

[

Security Council Election Flow

379×744 8.41 KB

](https://global.discourse-cdn.com/standard17/uploads/arbitrum1/original/2X/b/b98dd11c572099264860f4f13a6cb6754853073e.png)

Election Stages in detail

1. Nominee selection (7 days)

This stage consists of handling election timing, candidate registration, candidate endorsement:

- Election creation. Elections can be created by anyone, but only every 6 months. The election alternates between targeting the positions on the two cohorts. Once created, this first stage of the election process lasts for 7 days.

- Candidate registration. During these 7 days, any candidate can register, unless they are already a member of the other cohort. Members of the current cohort (the cohort up for election) are allowed to register for re-election.

- Endorsing candidates. Delegates can endorse a candidate during this 7 day window. A single delegate can split their vote across multiple candidates. No candidate can accrue more than 0.2% of all votable tokens.

- Fallback in case of too few candidates. In the event that fewer than 6 candidates receive a 0.2% endorsement, outgoing members of the cohort up for election will be selected to make up to 6 candidates.

Implementation details

The nominee selection process is implemented by the SecurityCouncilNomineeElectionGovernor contract.

It inherits most of its functionality from the Open Zeppelin Governor contracts and we have extended it with an extra feature:

- Custom counting module to allow delegates to endorse multiple candidates.

The governor contract has the following characteristics:

- A new proposal is created each election cycle, with an identifier unique to that election cycle.

- Candidates can the put themselves forward by calling addContender.

- Delegates can call castVoteWithReasonAndParams, supplying custom arguments in the params to indicate which candidate they wish to endorse with what weight.

2. Compliance check by the Foundation (14 days)

The Foundation will be given 14 days to vet the prospective nominees. If they find that a candidate does not meet the compliance check, they can exclude the candidate from progressing to the next stage. Note that grounds for exclusion could include greater than 3 members of a given organisation being represented in the nominee set (as described in section 4 of the Constitution).

Implementation details

The foundation can exclude a nominee by:

- Calling a custom excludeNominee function on the same SecurityCouncilNomineeElectionGovernor contract.

The Governor smart contract enforces the 2 week time period and the Foundation must exclude nominees by this deadline.

Once the compliance check has completed:

- Anyone can call the execute function on the SecurityCouncilNomineeElectionGovernor to proceed to the member election stage.

If there are less than 6 eligible nominees, then the Foundation will consult with outgoing members of the cohort on whether they will continue in this role for another 12 months. Members of the existing cohort may be selected at random to fill the remaining seats.

3. Member election (21 days)

The voting process can begin once a set of compliant candidates have been successfully nominated.

The voting process is designed to encourage voters to cast their vote early. Their voting power will eventually decay if they do not cast their vote within the first 7 days:

- 0 - 7 days. Votes cast will carry weight 1 per token

- 7 - 21 days. Votes cast will have their weight linearly decreased based on the amount of time that has passed since the 7 day point. By the 21st day, each token will carry a weight of 0.

Additionally, delegates can cast votes for more than one nominee:

- Split voting. delegates can split their tokens across multiple nominees, with 1 token representing 1 vote.

Implementation details

The Security Council member election will take place in a separate SecurityCouncilMemberElectionGovernor contract which will also inherit from Open Zeppelin Governor contracts.

After the 14 day waiting period for the compliance check, anyone can trigger a new member election:

- Call the execute function in SecurityCouncilNomineeElectionGovernor to deploy a new election proposal for SecurityCouncilMemberElectionGovernor

The SecurityCouncilMemberElectionGovernor includes:

- A custom counting module that allows delegates to split their vote and accounts for the linear decrease in voting weight.

- These additional parameters are supplied as the params argument when calling castVoteWithReasonAndParams.

- The custom counting module also checks that the nominee being voted is a compliant one by checking against the compliant nominee list in the SecurityCouncilNomineeElectionGovernor.

At the end of the 21 days of election:

- Anyone can call the execute function on the SecurityCouncilMemberElectionGovernor contract to initiate the update of top 6 nominees with the most votes into SecurityCouncilManager.

Update stages in detail

1. Security Council manager update

The security council manager is a contract which contains the canonical list of security council members, and which cohort they are part of. When a member election completes, the manager updates its local list of the current cohorts then forms cross chain messages to propagate those updates to each of the Security Council Gnosis safes.

The manager also provides some additional functionality to allow the security council to:

- Remove a member: As described in the Constitution, the council can remove one of its own members. The DAO can also remove a member under special conditions described by the Constitution.

- Add a member: After removing a member, the council can add a member

- Address rotation: As a practical matter, a council member can rotate one of their own keys. This can only be done with the approval of at least 9/12 council members as well as explicit approval from the member carrying out the rotation.

Implementation details

The manager functionality is contained within a custom SecurityCouncilManager smart contract. Since the SecurityCouncilManager is indirectly able to make calls to the standard UpgradeExecutor contracts which have far reaching powers, special care must be take to ensure the manager only makes council member updates.

Calling the UpgradeExecutors on each of the chains requires navigating withdrawals transactions, timelocks and inboxes, the SecurityCouncilManager outsources the calldata creation for these routes to a UpgradeExecRouteBuilder contract.

2. Timelocks and withdrawal

Constitutional DAO proposals all pass through:

- L2 timelock (3 days),

- L2 → L1 withdrawal (~7 days),

- L1 timelock (3 days).

You can read more about these stages in the governance docs. The purpose of these delays is to ensure that users wishing to withdraw their assets before the proposal is executed will have the time to do so. Changing the Security Council members should also provide this guarantee, so after the election has completed and before the Security Councils are updated the update message also goes through these same stages. The update message will use the existing timelocks to enforce these delays.

Implementation details

The existing governance timelock contracts are used as part of this flow.

The SecurityCouncilManager is given the PROPOSER role on the L2 timelock enabling it to create messages that will eventually be received by each UpgradeExecutor.

3. Individual council updates

The new Security Council members need to be installed into 4 Gnosis safes:

- Arbitrum One 9 of 12 Emergency Security Council

- Arbitrum One 7 of 12 Non-Emergency Security Council

- Ethereum 9 of 12 Emergency Security Council

- Nova 9 of 12 Emergency Security Council

The old cohort of members will be removed, and the new cohort will replace them.

Implementation details

To do this the existing [Upgrade Executor contracts](#) on each chain will be installed as Gnosis Safe modules into the Security Council safes. A custom [Governance Action Contract](#) will be used to call the specific OwnerManager addOwnerWithThreshold and removeOwner methods on the Gnosis safes.

Additional affordances

The Constitution also declares some other additional affordances to certain parties

1. The DAO can vote to remove a member prior to the end of their term, as long as 10% of possible votes are cast in favour and 5/6 of cast votes are in favour. This will be implemented as a governor with correct quorum and proposal passed thresholds. This governor will be given the rights to call removeMember on the SecurityCouncilManager.

2. The Security Council can remove a member prior to the end of their term, if 9 of 12 members agree. The 9 of 12 council will be given the rights to call removeMember on the SecurityCouncilManager.

3. The Security Council can add a member once one has been removed, if 9 of 12 members agree and if there are less than 12 members currently on the council. The 9 of 12 council will be given the rights to call addMember on the SecurityCouncilManager.

Constitution Updates

The proposed implementation mostly satisfies the specification outlined by the Arbitrum Constitution. There are some minor changes that are required to the Constitution's text to take into account the time it takes to install new candidates and to support compliance procedures set out by the Arbitrum Foundation.

Note, the final wording for how to update the Constitution will be provided in a later revision. We simply want to notify the requirement that the text needs to be changed. At this stage, our request for feedback is focused on the implementation details of the smart contract suite.

Update timeline for the election

The Section 4 of the Constitution contains the text:

- From T until T+7 days: Any DAO member may declare their candidacy for the Security Council; provided that a current Security Council member in one cohort may not be a candidate for a seat in the other cohort. To the extent that there are more than six candidates, each eligible candidate must be supported by pledged votes representing at least 0.2% of all Votable Tokens. In the event that fewer than six candidates are supported by pledged votes representing at least 0.2% of all Votable Tokens, the current Security Council members whose seats are up for election may become candidates (as randomly selected out of their Cohort) until there are 6 candidates.

- From T+7 days until T+28 days: Each DAO member or delegate may vote for any declared candidate. Each token may be cast for one candidate. Votes cast before T+14 days will have 100% weight. Votes cast between T+14 days and T+28 days will have weight based on the time of casting, decreasing linearly with time, with 100% weight at T+14 days, decreasing linearly to 0% weight at T+28 days.

- At T+28 days: The 6 candidates who have received the most votes are elected and immediately join the Council, replacing the Cohort that was up for re-election.

We need to make three changes to the Arbitrum Constitution:

- New timeline. A dedicated compliance process must be included between the nominee selection and member election phases. This will shift the timeline of events and the total election will now last at least 42 days alongside additional time to install the newly elected Security Council members via the on-chain governance smart contracts.

- Less than 6 eligible nominees. The Arbitrum Foundation has the authority to add new nominees during the Compliance stage if there are less than 6 eligible nominees.

- Installation time. We need to remove the phrase 'immediately join the Council' to take into account the on-chain governance process for installing the newly elected candidates. For example, the various time locks to protect a user's right to exit Arbitrum during the upgrade and the time it takes to send an L2 → L1 message.

With the above in mind, we propose an update to Section 4 of the Constitution with the following text:

- Nominee selection (T until T+7 days): Any DAO member may declare their candidacy for the Security Council; provided that a current Security Council member in one cohort may not be a candidate for a seat in the other cohort. To the extent that there are more than six candidates, each eligible candidate must be supported by pledged votes representing at least 0.2% of all Votable Tokens.

- Compliance process (T+7 until T+21 days): All candidates will cooperate with The Arbitrum Foundation and complete the compliance process. The Arbitrum Foundation is responsible for removing any candidates that fail the compliance process. In the event that fewer than six candidates are supported by pledged votes representing at least 0.2% of all Votable Tokens, the current Security Council members whose seats are up for election may become candidates (as randomly selected out of their Cohort) until there are 6 candidates.

- Member election (T+21 until T+42 days): Each DAO member or delegate may vote for any declared candidate. Each token may be cast for one candidate. Votes cast before T+28 days will have 100% weight. Votes cast between T+28 days and T+42 days will have weight based on the time of casting, decreasing linearly with time, with 100% weight at T+28 days, decreasing linearly to 0% weight at T+42 days.

- At T+42 days: The process for replacing the cohort of Security Council members with the 6 candidates who received the most votes will be activated. The installation process must be executed via the on-chain governance smart contracts and it may take several days until the new Security Council members are installed.

Compliance checks by the foundation.

The Constitution contains the text:

- "Prior to the next Security Council election, The Arbitrum Foundation shall establish and set forth more detailed procedures and guidelines regarding the election process for the Security Council, which may include, but aren't limited to, a candidate intake process in order to comply with Cayman Islands laws, a standard template for candidates to complete for purposes of their public nominations and other processes to ensure an orderly, fair and transparent election."

The text gives an affordance to the Foundation to conduct a compliance check on the potential nominees. We propose to make this check an explicit stage of 14 days between Nominee Selection and Member Election to allow the Foundation to conduct these checks. Details of compliance checks will be provided by the Arbitrum Foundation at a later date.

We propose to update the Constitution with the following text:

- The Arbitrum Foundation is allocated 14 days for the Compliance process and it should be executed between the Nominee selection and Member election. The Arbitrum Foundation has flexibility to update its compliance policy for every new election. This is required to allow The Arbitrum Foundation to comply with Cayman Island laws. Furthermore, The Arbitrum Foundation maintains the right to issue new procedures and guidelines for off-chain components of the Security Council election. All efforts should be made by The Arbitrum Foundation to ensure an orderly, fair, and transparent election.

Final update to the Constitution text.

For completeness, the amended text for Section 4 of the Arbitrum Constitution, including the changes from AIP-4:

The Security Council has 12 members, who are divided into two Cohorts of 6 members.

The initial Security Council Cohorts were determined by randomly splitting the 12 members into two 6-member cohorts - 6 members in the 'First Cohort' and 6 members in the 'Second Cohort'. The members of the initial Security Council Cohorts are detailed in a transparency report here.

The first Security Council election is scheduled to begin on the 15th September 2023 or the earliest possible date. The election can only begin upon the availability of an on-chain election process that is approved and installed by the Arbitrum DAO. This first election replaces the 'First Cohort'. The next election replaces the 'Second Cohort' and so forth.

The date chosen for the first election will form the basis for all future elections. Every election should begin 6 months after the previous election has started and it will replace its respective cohort of 6 members.

All Security Council members are expected to serve their term until the election is complete and the new Security Council members are installed.

The following timeline governs an election that starts at time T:

1. Nominee selection (T until T+7 days): Any DAO member may declare their candidacy for the Security Council; provided that a current Security Council member in one cohort may not be a candidate for a seat in the other cohort. To the extent that there are more than six candidates, each eligible candidate must be supported by pledged votes representing at least 0.2% of all Votable Tokens.

2. Compliance process (T+7 until T+21 days): All candidates will cooperate with the Arbitrum Foundation and complete the compliance process. The Arbitrum Foundation is responsible for removing any candidates that fail the compliance process. In the event that fewer than six candidates are supported by pledged votes representing at least 0.2% of all Votable Tokens, the current Security Council members whose seats are up for election may become candidates (as randomly selected out of their Cohort) until there are 6 candidates.

3. Member election (T+21 until T+42 days): Each DAO member or delegate may vote for any declared candidate. Each token may be cast for one candidate. Votes cast before T+14 days will have 100% weight. Votes cast between T+21 days and T+35 days will have weight based on the time of casting, decreasing linearly with time, with 100% weight at T+21 days, decreasing linearly to 0% weight at T+42 days.

4. At T+42 days: The process for replacing the cohort of security council members with the 6 candidates who received the most votes will be activated. The installation process must be executed via the on-chain governance smart contracts and it may take several days until the new security council members are installed.

The Arbitrum Foundation is allocated 14 days for the Compliance process and it should be executed between the Nominee selection and Member election. The Arbitrum Foundation has flexibility to update its compliance policy for every new election. This is required to allow The Arbitrum Foundation to comply with Cayman Island laws. Furthermore, The Arbitrum Foundation maintains the right to issue new procedures and guidelines for off-chain components of the Security Council election. All efforts should be made by The Arbitrum Foundation to ensure an orderly, fair, and transparent election.

As a matter of best practice for maintaining an independent Security Council, no single organisation should be overly represented in the Security Council. In particular, there should not be more than 3 candidates associated with a single entity or group of entities being elected to the Security Council, thereby ensuring that there will be no single entity or group of entities able to control or even veto a Security Council vote.

Furthermore, no candidate with conflicts of interest that would prevent them from acting in the best interests of the ArbitrumDAO, Governed Chains and/or The Arbitrum Foundation should be elected to the Security Council. Potential conflicts of interest could be, but are not limited to, affiliations with direct Arbitrum competitors, proven histories of exploiting projects and others.

The DAO may approve and implement a Constitutional AIP to change the rules governing future Security Council elections, but the AIP process may not be used to intervene in an ongoing election.

Security Council members may only be removed prior to the end of their terms under two conditions:

1. At least 10% of all Votable Tokens have casted votes "in favour" of removal and at least 5/6 (83.33%) of all casted votes are "in favour" of removal; or

2. At least 9 of the Security Council members vote in favour of removal.

The seats of Security Council members who have been removed prior to the end of their respective terms shall remain unfilled until the next election that such seats are up for appointment, unless otherwise replaced prior to such next election by a vote of at least 9 of the Security Council members, in which case such seat shall be up for appointment at the next such election. The Security Council may not re-appoint a removed member and they can only be re-elected via the election voting system.