BIC Process

The **Beanstalk Immunefi Committee**, **or BIC**, determines the categorization and payout of bug bounties in accordance with the bug bounty program structure approved by the Beanstalk DAO. The BCM executes the will of the BIC as determined by Beanstalk Immunefi Responses (BIRs), up to a maximum number of Beans approved via governance.

BIC Members serve as signers on the BIC Multisig (BICM), a 4-of-6 Safe multisig that is the sole wallet that can update the number of remaining Beans approved by the DAO to be minted for bug bounties.

The Immunefi Bug Bounty Program is focused preventing loss of Farmers' Beanstalk assets in Beanstalk and other ecosystem smart contracts.

You can read more about the current BIC Members and data on past Beans minted for bounties on the BICM Dashboard in the Farmers' Almanac.

Immunefi Program

You can read the full program and submit bug reports on the Immunefi Bug Bounty Program page. The latest version of the program approved by the DAO can be found on Arweave here.

In summary:

- The max bounty is 1,100,000 Beans;
- Immunefi takes a 10% fee in Beans on top of any bounty;
- Bugs are categorized as Critical, High or Medium severity;
- The BIC determines whether a whitehat is entitled to a bug bounty/reward, and if so, the amount of such bounty/reward according to the defined bug bounty program structure; and
- Immunefi serves as a mediator in cases where a whitehat disputes the BIC's determination of whether the whitehat is entitled to any bug bounty/reward, or what the appropriate bounty/reward should be within each Impact range.

Security is paramount to the success of Beanstalk. Immunefi is crypto's leading bug bounty platform that many other well-known DeFi protocols use to facilitate their bug bounty programs. This bounty program is competitive with the largest programs currently on Immunefi, making it likely to attract whitehat hackers.

This program establishes a method for the reporting and fixing bugs in a way that minimizes the risk to Beanstalk between the report and the fix, as well as the fair and transparent compensation for the reporting of bugs. The program gives bounty hunters a clear process and structure in order to increase the likelihood they attempt to find issues with Beanstalk and its related contracts and code.

The BIC structure of community-known members (see BICM Dashboard) and public Snapshot proposals (see Beanstalk Bug Bounty Snapshot page) allows the Beanstalk community to scrutinize decisions, while still allowing the BIC to move swiftly in response to bug reports. The BIC consists of technical members of the Beanstalk community due to the nature of the BIC. The BIC can keep the bug information private while the bug is unfixed, and then has a clear process to disclose the bug to the public and compensate the whitehat.

Having several members on the BIC increases decentralization. The two-thirds majority required to approve a BIR and the BCM minting the Beans introduces multiple steps to mint Beans as a reward, which improves censorship-resistance.

Multisig Powers

The BIR Beans Remaining contract has functions for increasing and decreasing the number of Beans remaining that can be minted per BIRs in order to reflect the will of the DAO. The BICM is the owner address that can call these functions. These functions should only be called after a proposal has passed.

The following functions on the BIR Beans Remaining contract are only callable from the owner address:

- `increaseRemainingBeans` — Increase the number of remaining Beans that can be minted for bug bounties.
- `decreaseRemainingBeans` — Decrease the number of remaining Beans that can be minted for bug bounties.
- `changeOwner` — Transfer ownership of the BIR Beans Remaining contract to a new address.

Responsibilities

The BIC has the following primary responsibilities:

- Following the processes outlined in ＃**Response Process**;
- Updating the BIR Beans Remaining contract to reflect the will of the DAO (see ＃**Multisig Powers**); and
- Updating the Immunefi Bug Bounty Program when necessary.

The BIC may update the Immunefi Bug Bounty Program in the following cases:

- Adding new assets as in-scope, particularly contracts that have been audited by Halborn and/or have attracted large amounts of Beans/BDV;
- Updating the list of pull requests whose code has been audited by Halborn, but has not yet been committed to Beanstalk;
- Adding documentation and links; and
- Updating language to improve clarity.

Any other changes to the Immunefi Bug Bounty Program require a BOP (or BIP).

Rotating Signers

In the event that one or more Signers are deemed unfit for the BIC (or a Signer voluntarily chooses to be removed from the BICM), the BICM will rotate them out of the multisig and replace them with a backup Signer approved by the DAO.

Response Process

The following outlines the process that the BIC follows upon receipt of a bug report.

Immediate Response

After a bug report is submitted through the Immunefi Dashboard, all BIC Members are notified via email.

As mentioned in the bug bounty program, in order to be considered for the maximum potential reward, bug reports must come with (1) a Proof of Concept (PoC), and (2) code implementing the fix.

In response to each bug report, the BIC will immediately:

- Forward the the bug report (and fix PoC if included in the bug report) to Halborn via the Bug Reports Slack channel; and
- Evaluate the validity and severity of the bug, as well as the fix PoC if included in the bug report.

Bug Fix

If it is determined that the bug report is invalid, the BIC will close the report on the Immunefi Dashboard.

If it is determined that the bug report is valid, the BIC will work with the corresponding party (the BCM, the Root DAO Multisig (RDM), etc.) to resolve the issue as soon as possible via an emergency upgrade. The fix will be forwarded to Halborn for review.

BIR Proposal

As soon as possible after completing the above, the BIC will prepare, but not publish, a BIR, which includes:

- Whether the bug report qualifies for a Critical, High or Medium Impact bounty/reward;
- What the potential practicable economic damage of the bug is (if categorized as Critical or High Impact);
- What the appropriate bounty/reward should be within the Impact range; and
- Whether the whitehat is entitled to a bug bounty/reward, and if so, the amount of such bounty/reward.

In instances where there are multiple bugs reported in the same report, a BIR will be prepared for each bug.

After preparing the BIR, the BIC will:

- Confirm the contents of the BIR with the whitehat via the Immunefi Dashboard (as outlined in the Immunefi Bug Bounty Program, in certain instances where the whitehat disputes the BIC's determination of the bug report, Immunefi mediates);
- Forward the following information to the BCM for their submission of the Safe transaction:
  - The whitehat's address;
  - The corresponding bounty amount in Beans;
  - Immunefi's address; and
  - The corresponding fee amount in Beans;
- Include a link to the Safe transaction in the BIR;
-

Include a **Beans Minted** section in the BIR that describes the number of Beans minted by the execution of the `diamondCut`;

- Publish the BIR on Snapshot;
- Announce the existence of the BIR to the community in the Beanstalk Discord; and
- Vote on the BIR.

BIR voting takes place on the Beanstalk Bug Bounty Snapshot page and lasts for 3 days. Only BIC members propose and vote on BIRs, and each member has one vote. BIC members can either vote For or Against a BIR, and a two-thirds majority of the BIC voting For is required to pass.

BIR Execution

Once a BIR passes, the BCM executes it by:

- Minting Beans corresponding to the bounty to the whitehat's address; and
- Minting Beans corresponding to the 10% fee to Immunefi's address.

The BICM will then call `decreaseRemainingBeans` on the BIR Beans Remaining contract in order to account for the newly minted Beans.