Disclaimer: Immunefi, Spearbit, and Nethermind are all aware of the current RFP process for security providers. We wanted to release the initial proposal we had created in order to raise awareness and receive feedback from the community. We all absolutely plan to participate in the RFP process. Let me know if there are further questions.

Team

Henry Shen

- BD/GTM at Immunefi
- hen@immunefi.com

Omar Bheda

- Head of Growth at Spearbit Labs
- omar@spearbit.com

Peter Kecman

- BD Lead at Nethermind
- peter@nethermind.io

Outline

This proposal dictates the agreement between Spearbit, Immunefi, and Nethermind as industry-leading security service providers across the web3 ecosystem to provide comprehensive bug coverage and security services to the Arbitrum ecosystem. This includes but is not limited to providing subject matter expertise from the best professionals in web3 security to conduct:

Spearbit & Nethermind

- Pre-deployment Security Advisory (Spearbit, Nethermind)
- Smart Contract Security Reviews / Audits (Spearbit, Nethermind)
- Web2 Security Reviews / Penetration Testing (via Cantina)
- Incident Response and Monitoring (Spearbit, Immunefi, Nethermind)
- Crowdsourced Security Competitions (via Cantina)
- Formal Verification / Specification (Spearbit, Nethermind)

Immunefi

- Robust Bug Bounty Programs
- On-chain Vaults for Payouts
- Fully Managed Triage Service

Motivation

The core motivation and purpose for driving comprehensive bug coverage and security review services beyond basic smart contract security services is to position protocols building on Arbitrum for operational excellence. We strongly believe that to maximize the security posture of the Arbitrum ecosystem a far more holistic and comprehensive approach to security is needed. We’ve highlighted these areas below and why we believe that providing full security coverage and advisory services from beginning to end will enable the Arbitrum ecosystem to scale far more quickly and efficiently.

vCISO Secure Development Advisory Services: This service aims to provide protocols and projects building on Arbitrum with subject matter experts in secure web3 development lifecycles in the form of a virtual CISO or external consultant that can focus on system architecture and guide development teams towards security best practices. Spearbit and Nethermind have provided similar advisory services to other leading protocols such as Optimism, Worldcoin, and Polygon ID to re-evaluate complex design choices or architecture from a security mindset. These technical advisory services are best represented anecdotally by:

“an ounce of prevention is worth a pound of cure”

Smart Contract Security Reviews / Audits: We intend to provide comprehensive and high-signal bug coverage of Arbitrum protocols through protocol security reviews by industry-leading security researchers/auditors. Spearbit, Immunefi, and Nethermind are home to many of the top 50 web3 security professionals in the ecosystem and are ready at a moment’s notice to employ the absolute best talent available to secure mission-critical protocols building on Arbitrum. With each partner providing their unique approach to security audits, we will further ensure that Arbitrum ecosystem projects have diverse security options to choose from. We believe industry-leading protocols deserve no less than the best security talent available, and we vouch to provide this for the Arbitrum ecosystem.

Web2 Security Reviews / Penetration Testing: With the advent of numerous protocols and projects being exploited by traditional attack vectors, it has become evident and increasingly clear that there is a pressing need to address the security concerns inherent in the traditional web2 frameworks that protocols are utilizing within the web3 ecosystem. In addition to provisioning comprehensive smart contract security solutions and coverage, we believe in providing full-suite application, cloud, and network penetration testing.

Incident Response and Monitoring: Through harnessing advanced analytics and deep blockchain expertise, this service provides real-time surveillance of web3 ecosystems to detect and mitigate potential threats. In the event of an anomaly or breach, we can provide rapid incident response measures with swift remediation, safeguarding your assets and reputation. We want to enable all builders on Arbitrum to navigate the web3 landscape with confidence, knowing that they are backed by the pinnacle of security vigilance and response readiness with Spearbit, Immunefi and Nethermind.

Crowdsourced Security Competitions: Through Cantina, a web3 security platform incubated by Spearbit, protocols can conduct crowdsourced security competitions to maximize the value added to their security posture by optimizing for maximum code coverage with high-signal security findings and less spam.

Bug Bounty Programs: Bug Bounty Programs allow projects to leverage security researcher communities to improve their protocol's security over a continuous period of time. The core aspect of a bug bounty program is the bug bounty, which is a financial reward given to security researchers in exchange for any known vulnerabilities. Bug Bounty Programs are vital to a project's risk management strategy and should always be implemented as a last, added layer of security.

Formal Verification: Formal verification can identify flaws that could potentially lead to exploits before our clients' smart contracts are deployed. Nethermind's formal verification team works in tandem with project engineering teams to define a standard specification detailing the behaviors of their smart contracts. Once defined, our formal verification experts can verify that the implementation satisfies these specifications. Furthermore, Nethermind Security has expertise in developing Interactive Theorem Proving (ITP) infrastructures and Automated Theorem Proving (ATP) tools, enabling us to reason about smart contracts precisely.

Rationale

Spearbit, Immunefi, and Nethermind are teaming up together to provide comprehensive security services and bug coverage for the entire Arbitrum ecosystem, given our track records within the Arbitrum ecosystem and other ecosystems like Optimism, zkSync, and Starknet. We also wholeheartedly believe that receiving diverse feedback and opinions is paramount to an ecosystem's security posture. Spearbit has work experience and a track record in many other ecosystems and with core actors such as Optimism, Polygon, Coinbase, zkSync, OpenSea and many others. Immunefi also works with other notable ecosystems, such as Optimism, Avalanche, Polygon, LayerZero, Scroll, etc., in hosting bug bounty for their protocols and Dapps. Nethermind, with its core development, infrastructure, cryptography research, development, and security expertise, provides a unique mix of skill sets that is hard to come across in a single organization. Their partners include the likes of Ethereum Foundation, Starknet, Gnosis Chain, Lido, Obol, and many others, with Nethermind Security being one of the leading security auditors in the StarkNet ecosystem, as well as working with Polygon, zkSync, and Worldcoin, among others. Our 35,000+ security researcher community does not discriminate against any type of project, allowing Arbitrum projects to receive diverse opinions and feedback from various types of security researchers worldwide. Immunefi is able to run a bug bounty program for any type of project (defi vs. consumer-facing Dapp) regardless of ecosystem or coding language (ETH, Cosmos, Avalanche, etc).

As mentioned earlier, Immunefi is currently working with the Arbitrum Foundation/Offchain Labs team to run an Immunefi bug bounty program for the Arbitrum protocol itself. Immunefi currently provides comprehensive bug coverage to 22 Arbitrum projects and has identified at least 5 other Arbitrum projects that are onboarding onto Immunefi in the near future. These 22 Arbitrum projects have received a total of 930 bug reports, with 118 bug reports resulting in a payout to a security researcher. Out of the 118 paid bug reports, 18 paid bug reports were labeled as critical, meaning that the bug identified would have resulted in direct theft of funds or protocol insolvency. The total cumulative payout amount across these 22 Arbitrum projects totals $2.2M USD to date.

Overview of Stakeholders

Spearbit: Spearbit is a distributed network of industry-leading security researchers tackling the most complex and mission-critical protocols across web3. We provide smart contract security services for industry-leading protocols and actors such as Optimism, OpenSea, Polygon, Coinbase, zkSync, and many more.

Spearbit has:

- Actively protected 4B+ in TVL
- Paid out 13M+ to its Security Researchers
- 40+ Lead Security Researchers

- Christoph Michel (cmichel)
- Liam Eastwood (0xLeastwood)
- Gerard Persoon
- Zach Obront
- Kurt Barry
- 0x52
- Peter Kacherginsky
- Eduard Sanou
- Carlos Perez Baro (cperezz.eth)
- (Radek)
- Evan Laufer
- Aditya Shishir Asagonkar
- Francesco Damato (fradamt)
- Parithosh Jayanthi
- Dmitry Artimenia (Dmitriia)
- Nirvan Tyagi
- Wilson Nguyen
- Andrei Maiboroda
- Riley Holterhus (holterhus)
- Yoav Weiss (yoavw)
- Saw-mon and Natalie
- Rajeev Gopalakrishna (Rajeev | Secureum)
- Noah Marconi (ndev)
- Ho Wei Lun Desmond (hickup)
- Jonah1005
- Guido Vranken
- William Pote
- Optimum
- Emanuele Ricci (stermi)
- Thibaut Schaeffer
- Pawel Bylica
- Christian Reitwiessner (chriseth)
- Leonardo de Sa Alt
- Brock Elmore
- lightclient
- D-Nice
- Mudit Gupta

- Harikrishnan Mulackal (hrkrshnn)
- Alex Beregszaszi (axic)
- shw
- 100+ Security Researchers with robust talent gates
- Christoph Michel (cmichel)
- Liam Eastwood (0xLeastwood)
- Gerard Persoon
- Zach Obront
- Kurt Barry
- 0x52
- Peter Kacherginsky
- Eduard Sanou
- Carlos Perez Baro (cperezz.eth)
- (Radek)
- Evan Laufer
- Aditya Shishir Asagonkar
- Francesco Damato (fradamt)
- Parithosh Jayanthi
- Dmitry Artimenia (Dmitriia)
- Nirvan Tyagi
- Wilson Nguyen
- Andrei Maiboroda
- Riley Holterhus (holterhus)
- Yoav Weiss (yoavw)
- Saw-mon and Natalie
- Rajeev Gopalakrishna (Rajeev | Secureum)
- Noah Marconi (ndev)
- Ho Wei Lun Desmond (hickup)
- Jonah1005
- Guido Vranken
- William Pote
- Optimum
- Emanuele Ricci (stermi)
- Thibaut Schaeffer
- Pawel Bylica
- Christian Reitwiessner (chriseth)
- Leonardo de Sa Alt

- Brock Elmore
- lightclient
- D-Nice
- Mudit Gupta
- Harikrishnan Mulackal (hrkrshnn)
- Alex Beregszaszi (axic)
- shw
- 100+ Security Researchers with robust talent gates

Immunefi: Immunefi is a Web3-focused bug bounty platform that protects over $60 billion in user funds. We work with many notable names across L1s, L2s, DeFi protocols (such as LayerZero, Cronos Labs, Polygon, Arbitrum, Boba Network, GMX, SushiSwap, etc.) in hosting bug bounties for their protocols. We host bug bounties for any type of blockchain project, regardless of coding language, ecosystem, or type of project (defi vs. creator economy). We utilize a community of over ~35k security researchers who use our platform to hunt for bugs within our clients' protocols.

Nethermind: Nethermind is a blockchain research and software engineering company empowering enterprises and developers worldwide to work with and build upon decentralized systems. Our work touches every part of the web3 ecosystem, from core development and fundamental cryptography research through security to application-layer protocol development. As one of the core contributors to the development of Ethereum, our execution client represents a significant portion of synced nodes. In addition, we are active builders of the Starknet ecosystem, delivering a node implementation, block explorer, Solidity-to-Cairo transpiler, and formal verification tooling.

With our agile and academic approach to smart contract security, we have established Nethermind Security as a leading auditor in the Starknet ecosystem. Furthermore, we have been working with a number of leading actors in the Ethereum ecosystem, such as zkSync, Gnosis Chain, Polygon ID, Worldcoin, Risc Zero, Gyroscope, and others. Nethermind Security utilizes the experience and knowledge of other teams within Nethermind, such as the research team, smart contract development team, and protocol engineering team, among others. As of now, Nethermind employs over 220 professionals.

Nethermind Security has:

- Reviewed over 100.000 LoC
- Discovered over 1000 issues
- With over 10% of High or Critical severity
- Over 50% of experts holding a Ph.D. degree
- Published 150+ scientific articles
- Holding 1,500+ citations in Google Scholar
- With over 10% of High or Critical severity
- Over 50% of experts holding a Ph.D. degree
- Published 150+ scientific articles
- Holding 1,500+ citations in Google Scholar

Key Terms

Secure Development Advisory Services: An industry-leading security expert in the secure web3 development lifecycle will be assigned to designate focused attention to the architecture and development of a protocol before launching.

Smart Contract Security Reviews / Audits: A comprehensive review of your protocols' architecture, including smart contracts and dependencies.

Web2 Security Reviews / Penetration Testing: A review of your traditional infrastructure, including any web applications, frontends, network architecture, and any other relevant endpoints comprising your web2 infrastructure.

Incident Response and Monitoring: A service offering real-time monitoring and threat mitigation in web3 ecosystems using advanced analytics and blockchain expertise. With prompt action to anomalies or breaches, we protect your assets and reputation, ensuring you can operate Web3 securely and with peace of mind.

Crowdsourced Security Competitions: A crowdsourced security review conducted through Cantina, seeking to maximize code coverage and leverage as many eyes as possible in order to perform a security review.

Cantina: An efficient web3 security marketplace incubated by Spearbit that provides protocols with full transparency and access to top web3 security service providers as well as high-signal crowdsourced security reviews called competitions.

Bug Bounty: A bug bounty is a financial or monetary reward given to security researchers for successfully discovering and reporting a vulnerability to the project's developer.

Bug Bounty Program: A program that allows projects to leverage security researcher communities to improve their protocols' security posture over a continuous time period.

Security Researcher: Skilled computer experts who use their technical knowledge and expertise to identify vulnerabilities within a project.

Managed Triage Service: A 24/7 premium Immunefi service that allows projects to reduce the time and effort spent reviewing and triaging bug reports.

Formal Verification: Formal verification is a rigorous method to mathematically prove or confirm the correctness of software systems through exhaustive analysis based on logical rules and models, ensuring their adherence to specified requirements or properties.

Specifications

Spearbit, Immunefi, and Nethermind are teaming up together to provide comprehensive security services and bug bounty coverage for mission-critical projects and applications.

Spearbit and Nethermind will be focused on providing a comprehensive "Swiss-cheese" approach to security for Arbitrum protocols, as shown below:

[

Screenshot 2023-12-06 at 2.15.09 PM

860×1072 39.1 KB

](https://global.discourse-cdn.com/standard17/uploads/arbitrum1/original/2X/0/00b2ae66b6565e7f74aa73f95d9b2fa59bd53fb1.jpeg)

Specific examples of Spearbit provided services:

- vCISO Advisory - Optimism Critical Bedrock Upgrade
- https://hackmd.io/@spearbit/BJXzIlwTq
- https://hackmd.io/@spearbit/BJXzIlwTq
- Smart Contract Security Review Portfolio
- GitHub - spearbit/portfolio
- GitHub - spearbit/portfolio
- Web2 Security Review
- OpenSecurity: Why Web2 Security is a necessity for Web3 Protocol… — Cantina
- OpenSecurity: Why Web2 Security is a necessity for Web3 Protocol… — Cantina
- Incident Response & Monitoring
- We've worked with several notable projects to build their comprehensive incident response and monitoring plans, but can not share it currently due to security concerns
- We've worked with several notable projects to build their comprehensive incident response and monitoring plans, but can not share it currently due to security concerns
- Competitions
- Competitions | Cantina
- Competitions | Cantina

Specific examples of Nethermind provided services:

- Smart Contract Security Review Portfolio
- GitHub - NethermindEth/PublicAuditReports: Public reports for audits done by Nethermind
- GitHub - NethermindEth/PublicAuditReports: Public reports for audits done by Nethermind
- Formal Specification
- PublicAuditReports/NM0069-FINAL_POLYGON_ID.pdf at main · NethermindEth/PublicAuditReports · GitHub
- PublicAuditReports/NM0058-FINAL_ZKLEND.pdf at main · NethermindEth/PublicAuditReports · GitHub
- PublicAuditReports/NM0069-FINAL_POLYGON_ID.pdf at main · NethermindEth/PublicAuditReports · GitHub
- PublicAuditReports/NM0058-FINAL_ZKLEND.pdf at main · NethermindEth/PublicAuditReports · GitHub
- General links:
- Smart contract audits | Secure auditing solutions
- Formal Verification | Solutions across three key areas
- Formal Verification | Solutions across three key areas
- Smart contract audits | Secure auditing solutions
- Formal Verification | Solutions across three key areas
- Formal Verification | Solutions across three key areas

Immunefi will be focused on providing any services that are related to bug bounties and bug bounty payouts. Some specific examples of these Immunefi-provided services are the bug bounty platform offering, on-chain vaults for payouts, and managed triage services for incoming bug reports.

The roles of this team include but are not limited to:

Cantina: Under Cantina, Spearbit and Nethermind will operate as guilds to provide security services to relevant core protocols across the Arbitrum ecosystem. Cantina will also provide Web2 security expertise, incident response, monitoring, and reviewing for any other unique additional attack surfaces or vectors that are requested by the Arbitrum ecosystem.

Spearbit: Will conduct extensive end-to-end security reviews for core protocols building on the Arbitrum ecosystem to identify core issues and bugs that may arise in any and all attack surfaces. Spearbit will also provide advisory services to protocols pre-deployment to bake in security into the development life cycle.

Immunefi: Will provide end-to-end bug bounty coverage and services for the Arbitrum protocol and any Arbitrum projects. Aside from bug bounty services, Immunefi will also report bug bounty payouts on a monthly basis. These monthly reports will contain additional details, such as the amount of TVL protected, bug bounty payout amount, etc, to showcase Immunefi's impact and the transparency of how grant funds are being used.

Nethermind: Will conduct thorough reviews of smart contracts to identify vulnerabilities and weaknesses in the code that could compromise the security or functionality of Arbitrum projects. Nethermind Security team will work closely with your project team via multiple sync calls and communication channels to ensure the audit is completed efficiently and effectively. The project team will have full visibility of the audit process, and findings will be discussed on the go, so projects can start working on the fixes as soon as we find a problem. We are taking an agile approach to our auditing process, enabling our team to deliver value to our clients much faster and with increased transparency.

Our smart contract audit service includes the following:

- A comprehensive review of your smart contract code
- Identification of vulnerabilities and weaknesses in the code
- Recommendations for improving the security and functionality of the smart contracts
- A detailed report outlining our findings and recommendations

Moreover, we can also provide the following:

- Formal Verification / Specification
- Performance reviews and recommendations for gas efficiency improvement
- In-depth analysis of the test suite

- Implementing fuzzing tests, white-box tests, and black-box tests
- Developing solutions for monitoring smart contracts in real-time using the Forta network

Costs

The total amount of funds we are requesting for this proposal is $5M, payable in ARB tokens. $3M will be allocated towards Cantina and $2M will be allocated towards Immunefi. For simplicity's sake, if we receive a total grant of $5M, Cantina will receive $2.4M for any security/auditing services to provide it's guilds (Spearbit + Nethermind) each receiving $1.2M, Cantina receiving $600K, while Immunefi will receive the remaining $2M for any bug bounty program services and payouts. Please refer to the following for a cost breakdown and justification for each party:

Immunefi:

- $2M USD (payable in ARB) for any bug bounty program-related services. We justify this number since we have paid out USD $2.2M in bug bounty rewards to date. As we onboard additional Arbitrum projects, we expect this payout figure to increase much faster, hence why we are asking for $2M USD.
- $1.59M USD (payable in ARB) will match critical or high bug bounty payouts for any Arbitrum projects with an Immunefi bug bounty program. For example, if GMX (already live on Immunefi) pays out $100K for a critical bug report, we will use $100K of the $1.4M to match this payout, doubling the critical reward payout. This will attract more security researchers to the Arbitrum ecosystem as we are effectively doubling their reward payouts and incentives
- ~$160K USD (payable in ARB) will be used for Immunefi's 10% fee that is charged on top of all bug bounty payouts. With the same GMX example above, the security researcher would receive a total reward of $200K USD (50% from GMX, 50% from this grant). This means that Immunefi would charge a fee of $20K USD (10% of $200K) on top of the bug bounty payout; however, $10K USD (50%) of this fee would be paid by GMX since they are paying half of the reward. This means that Immunefi would take the remaining $10K USD (remaining 50%) out of this grant. Immunefi charges a 10% fee on top of all bug bounty payouts since we have full-time staff actively working to manage and improve our bug bounty platform offering (including myself!)
- $250K USD (payable in ARB) for Immunefi's managed triage service. We will be providing a premium managed triage service for the 22 live Arbitrum programs on Immunefi and 5 onboarding Arbitrum projects to ensure that any valid bug report admissible for a matching payout is vetted correctly. We justify this number since the list price of our most basic, entry-level triaging service is $24K USD per year. Since we will technically manage 27 programs, the total market rate we normally charge would be $648K USD per year. This reflects a 61.4% discount rate from our original list price and market rate. All in all, we are discounting more than 60% to provide this service to the Arbitrum ecosystem.

Cantina:

- $600K (payable in ARB) to provision crowdsource security reviews in the form of competitions for Arbitrum protocols. Cantina will conduct 4-6 security competitions to maximize bug coverage from our talent pool where hundreds of security researchers review the same codebase competing to identify vulnerabilities.

Spearbit:

- $1.2M (payable in ARB) for providing a blended estimated rate based upon the Spearbit tiered security researcher rates:
- Lead Security Researchers - $20,000 USD
- Security Researchers - $12,500 USD
- Associate Security Researchers - $6,250 USD
- Junior Security Researchers - $3,000 USD
- Lead Security Researchers - $20,000 USD
- Security Researchers - $12,500 USD
- Associate Security Researchers - $6,250 USD
- Junior Security Researchers - $3,000 USD
- Spearbit will allocate a minimum of 1 LSR to each smart contract security review along with other security researchers. Assuming Spearbit employs a team of 4-5 security researchers on security reviews where there are:
- 1 LSR - $20,000 USD
- 1 SR - $12,500 USD

- 2 ASRs - $6,250 USD
- 1 JSR - $3,000 USD
- 1 LSR - $20,000 USD
- 1 SR - $12,500 USD
- 2 ASRs - $6,250 USD
- 1 JSR - $3,000 USD

The weekly average security review cost from Spearbit in turn will be $48,000 weekly. This number is subject to change or fluctuate depending on the needs of the protocol. Using this as a base, we can anticipate performing 25 weeks of comprehensive security reviews leveraging the best talent web3 security has to offer. Assuming each security review will span 2.5 weeks, this results in 10 security reviews by Spearbit for core Arbitrum protocols.

Nethermind:

- $1.2M (payable in ARB) for providing:
- 150 auditor weeks
- At the cost of $8.000USD per auditor per week.
- 150 auditor weeks
- At the cost of $8.000USD per auditor per week.
- Nethermind will allocate 3 auditors per audit, lasting on average 2-3 weeks. We expect to provide between 20 and 25 audits at the cost of $1.2M. For any other aforementioned services the same rate of $8.000USD per person per week applies

Distribution of Funds

We are proposing that the grant funds are distributed to each party in multiple installments of $250K USD (payable in ARB). Every incremental grant distribution after the first installment is based upon previous milestones that each individual party is responsible for attaining. Said party is also responsible for keeping track and delivering results to the DAO. Please refer to the following breakdown for additional details on milestones and distribution for each party:

Immunefi:

- Since Immunefi is already providing bug bounty program services for 22 live Arbitrum projects, we are requesting our first installment to be $500K USD (payable in ARB). 50% of the first installment ($250K USD) will be allocated towards the managed triage service described above. The remaining 50% ($250K USD) will be allocated towards bug bounty payouts and Immunefi fees for these payouts. That leaves a total remaining grant amount of $1.5M USD, which will be distributed in 6 additional installments of $250K USD. Each distribution after the initial installment will be based upon how much of the remaining funds are left for bug bounty payouts and Immunefi fees. For example, once the initial installment of $250K USD for bug bounty payouts and Immunefi fees hits a threshold of $100K USD, we will request our second installment to ensure there are enough funds to incentivize security researchers to continue hunting.

Cantina:

- Cantina will receive the 3M total over time and will operate as the recipient and distributor of funds to both Spearbit and Nethermind. Cantina is requesting to receive the installments in installments. For Payment #1

, we request 600K USD up front for 200K USD to be reserved for the first Arbitrum competitions on Cantina for protocols as well as 200K USD distributed each to Spearbit and Nethermind for protocol security reviews.

The rest of the payments can be as follows:

- Payment #2

to Cantina: 600K USD

- 200K USD to Cantina
- 200K USD to Spearbit
- 200K USD to Nethermind
- 200K USD to Cantina

- 200K USD to Spearbit
- 200K USD to Nethermind
- Payment #3

to Cantina: 600K USD

- 200K USD to Cantina
- 200K USD to Spearbit
- 200K USD to Nethermind
- 200K USD to Cantina
- 200K USD to Spearbit
- 200K USD to Nethermind
- Payment #4

to Cantina: 600K USD

- 300K USD to Spearbit
- 300K USD to Nethermind
- 300K USD to Spearbit
- 300K USD to Nethermind
- Payment #5

to Cantina: 600K USD

- 300K USD to Spearbit
- 300K USD to Nethermind
- 300K USD to Spearbit
- 300K USD to Nethermind