U.S. NATIONAL SCIENCE FOUNDATION
2415 EISENHOWER AVENUE
ALEXANDRIA, VIRGINIA 22314

NSF 25-027

Frequently Asked Questions (FAQs) for the NSF Safety, Security, and Privacy of Open-Source Ecosystems (Safe-OSE) Program (NSF 24-608)

eligible for Safe-OSE? Are there expectations regarding the level of adoption of the open-source product or how critical it is within other infrastructure?

12. Can my organization submit a proposal if we want to address vulnerabilities in a mature OSE managed by another organization?
13. Our product has known, unaddressed vulnerabilities. We intend to make the product available as open-source once these vulnerabilities are addressed. Would we be eligible for Safe-OSE funding?
14. We are a small, for-profit business that sells a product containing open-source components. Can we obtain Safe-OSE funding to test for vulnerabilities in those components and develop workarounds for our product?
15. Can an open-source product be owned by a for-profit organization, or must the managing organization be a non-profit?
16. Our ecosystem pertains to an open standard rather than a specific piece of open-source technology (such as software). Would we be eligible for Safe-OSE funding?
17. Our open-source project has a large backlog of identified security issues – too many for our developer team to manage. Would our project be eligible for Safe-OSE?
18. The solicitation states a limitation of two proposals per organization. Would being listed as a sub-awardee be considered the same as a proposal a lead institution?
19. Are the budget limits of $500,000 for the first year and $1,500,000 for the second year inclusive of indirect costs?
20. Is the second year of funding contingent on the success of the first year's goals or is it competitive with the project status of other grantees?
21. What are the appropriate roles of collaborators on a Safe-OSE project?
22. If our open-source product has government users, should we seek letters of collaboration from them?
23. Should sub-awardees submit Letters of Collaboration?
24. Can I sign up as a reviewer for the Safe-OSE program?
25. How long will it take for my proposal to be reviewed?
26. Do Letters of Collaboration need to follow the NSF *Proposal & Award Policies & Procedures Guide (PAPPG)* standard format for letters?

PROGRAM BASICS

1. **What is the goal of the Safety, Security, and Privacy of Open-Source Ecosystems (Safe-OSE) program?**

   The goal of the Safe-OSE program is to address significant safety, security, and/or privacy vulnerabilities (both technical and socio-technical) in open-source ecosystems (OSEs).

2. **What is the difference between Safe-OSE and the Pathways to Enable Open-Source Ecosystems (POSE) program?**

   The goal of the POSE program is to harness the power of distributed open-source development as an engine of innovation to address challenges of national and societal importance. POSE Phase I awards accomplish this goal by scoping and planning an OSE-managing organization while POSE Phase II awards aim at developing the OSE-managing organization and the ecosystem that surrounds it.

   In contrast, the Safe-OSE program presumes that a mature and capable OSE-managing organization already exists and has as a core goal improving safety, security, and/or privacy for the open-source products managed by that organization.

3. **Does a Safe-OSE proposal need to address all three aims (safety, security, and privacy)?**

   Safety, security, and privacy of products and systems are often inextricably connected. Nonetheless, a Safe-OSE proposal may focus on any subset of these goals as appropriate to the threat landscape of the open-source product in question.

4. **The Safe-OSE solicitation includes privacy issues as one of the three aims of the program. Are there specific classes of privacy issues that are targeted?**

   Privacy is a broadly used term referring to the protection of sensitive information. How privacy issues manifest themselves depends on the nature of the technology in question and the data processed by that technology. The key concern to address in a Safe-OSE proposal is how the specific privacy issue you expect to address will enhance the broader impacts of your open-source product.

5. **We want to study attacks and vulnerabilities for open-source software. Can Safe-OSE fund this work?**

   No. Safe-OSE is not a research-focused program. Consult the Dear Colleague Letter: Inviting Proposals to Open-Source Software Security to the Security and Trustworthy Cyberspace Program (NSF 23-149) for information about research support for topics

related to open-source software security.

6. **My organization has a security solution designed to be applicable across a broad set of open-source products. Can we get funding to offer this solution to many open-source projects, or must a Safe-OSE proposal need to focus on security, safety, and privacy issues specific to one specific ecosystem?**

   The Safe-OSE solicitation is designed to receive proposals from a managing organization that is responsible for the ecosystem of one open-source product or a closely connected suite of such products. Project activities must directly focus on improving the defenses and resiliency of that specific ecosystem.

7. **Is the Safe-OSE solicitation exclusively about security or is it also about related issues such as software quality and/or system performance?**

   Safe-OSE focuses on funding project activities that will fundamentally improve the safety, security, and/or privacy status of the managed product(s) as well as increase an ecosystem's resiliency to future attacks. Some of the mitigation processes funded by a Safe-OSE award may also have the beneficial side effect of improving software quality or system performance, but the primary focus of funded activities must be on safety, security, and/or privacy.

8. **Are basic authentication and authorization capabilities in scope or is the Safe-OSE solicitation just for protection against possible exploitable vulnerabilities?**

   The solicitation was written with the expectation that addressing safety, security, and/or privacy issues would enhance the broader impacts of an open-source ecosystem. Broader impacts can be enhanced through a variety of strategies that reduce the likelihood and/or impact of risks related to safety, security, and/or privacy. For example, a proposal could describe how establishment or improvement of authentication or authorization mechanisms would improve broader impacts.

9. **Does the scope of the Safe-OSE program include defining requirements or only the development tasks needed to improve safety, security, and/or privacy?**

   The solicitation was created with the expectation that, "Proposals to this program should provide clear evidence that OSE team leaders have established a thorough understanding of the threat landscape, vulnerabilities, and/or failure modes for the open-source product(s) managed by the OSE." A proposal focused primarily on defining, locating, exploring, or detecting vulnerabilities would not be in scope. The bulk of the expenditures in the project proposal should budgeted to activities that directly re-mediate known, understood vulnerabilities.

ELIGIBILITY

10. **What is the definition of a "mature" ecosystem in the context of the SAFE-OSE program?**

    A mature ecosystem comprises an effective managing organization that serves users, developers and other stakeholders; an impactful open-source product that is already in wide use and that has a capable developer community; infrastructure and tooling to support distributed development; administrative, legal, and governance capacity appropriate to the ecosystem; and mechanisms for long term sustainability. Ecosystems that have not reached this stage should consider submitting a proposal to the Pathways to Enable Open-Source Ecosystems (POSE) program.

11. **How large or how many users must the open-source product be, at a minimum, to be eligible for Safe-OSE? Are there expectations regarding the level of adoption of the open-source product or how critical it is within other infrastructure?**

    The solicitation does not specify a lower limit for the size of the user base. Merit reviewers will evaluate the broader impacts of the project based not only on the number of users, but also on the societal benefits of the open-source product, the number of other products and/or services dependent on the product in question, and the risks involved in security, privacy, and/or safety failures of the product.

12. **Can my organization submit a proposal if we want to address vulnerabilities in a mature OSE managed by another organization?**

    The solicitation was developed under the assumption that the OSE-managing organization is typically in the best position to understand the architecture of their product, the threat landscape, and the most efficient methods of addressing vulnerabilities. If a proposal is received from an organization that is not the OSE-managing organization for the product in question, the proposal would need to provide clear evidence that the proposers have the knowledge, experience, and access necessary to conduct a vulnerability remediation project effectively. Examples of such evidence could include, but are not limited to, involving the OSE-managing organization as a sub-awardee, submitting a letter of collaboration provided by the OSE-managing organization, and budgeting for involvement of senior project personnel who have "maintainer's privileges" (or equivalent capabilities) for the product in question. The proposal should also include a rationale describing why the OSE-managing organization did not serve as lead proposer on the project.

13. **Our product has known, unaddressed vulnerabilities. We intend to make the product available as open-source once these vulnerabilities are addressed. Would we be eligible for Safe-OSE funding?**

No. The Safe-OSE solicitation was developed so that mature, capable OSE-managing organizations could address vulnerabilities in existing open-source products. If your product is not yet available under an open-source license, it is likely that you have not yet had a chance to scope the ecosystem and/or develop a mature and capable managing organization. Consider submitting a proposal to the Pathways to Enable Open-Source Ecosystems (POSE) program instead.

14. **We are a small, for-profit business that sells a product containing open-source components. Can we obtain Safe-OSE funding to test for vulnerabilities in those components and develop workarounds for our product?**

    No. The Safe-OSE solicitation was developed so that OSE-managing organizations could address vulnerabilities in their own open-source products. The program is not intended to improve the marketability of a product sold by a for-profit firm. As a "downstream user" of an impactful open-source component, a for-profit firm could be involved in a Safe-OSE project that addresses the safety, security, and privacy of an open-source component. Contact the OSE-managing organization and alert them to the Safe-OSE program.

15. **Can an open-source product be owned by a for-profit organization, or must the managing organization be a non-profit?**

    Yes. As long as the product in question is licensed as open source, the solicitation allows for a variety of submitting organization types. See the Eligibility Information / Who May Submit Proposals section of the solicitation for more details.

16. **Our ecosystem pertains to an open standard rather than a specific piece of open-source technology (such as software). Would we be eligible for Safe-OSE funding?**

    Possibly. The solicitation is intentionally open-ended with respect to the nature of the open-source artifact that is addressed by proposals: "open source also refers to a range of publicly distributed products that transcend OSS [open source software], including scientific methodologies, models, and processes; manufacturing processes and process specifications; materials formulations; programming languages and formats; hardware instruction sets; system designs or specifications; and data platforms." Safe-OSE proposals must make a clear case that the remediation activities will address vulnerabilities that are presently inhibiting the intended broader impacts of the OSE.

17. **Our open-source project has a large backlog of identified security issues – too many for our developer team to manage. Would our project be eligible for Safe-OSE?**

No. The solicitation specifically mentions that Safe-OSE funding is not intended for "readily resolvable, known bugs." If an ecosystem has a capable community of developers, but the volume of bugs exceeds the capacity of that community, then a Safe-OSE proposal would need to address the origins of the mismatch and make a clear case that the proposed improvements would improve long-term resiliency.

18. **The solicitation states a limitation of two proposals per organization. Would being listed as a sub-awardee be considered the same as a proposal a lead institution?**

    A lead organization cannot submit more than two preliminary proposals. The solicitation does not place a limit on the number of times that an institution appears as a sub-awardee

PROGRAM DETAILS

19. **Are the budget limits of $500,000 for the first year and $1,500,000 for the second year inclusive of indirect costs?**

    Yes. Safe-OSE funding limits are inclusive of indirect costs. For organizations that do not have a negotiated indirect cost rate agreement (NICRA) with a federal government agency, check the solicitation for the use of a de minimis indirect cost rate.

20. **Is the second year of funding contingent on the success of the first year's goals or is it competitive with the project status of other grantees?**

    Second-year funding is contingent on achievement of first-year goals. The solicitation describes a reverse site visit process where a funded project will be evaluated based on achievement of agreed-upon first-year milestones. When an award is issued, the terms and conditions of the cooperative agreement will provide additional details about the timeline and expectations of the evaluation process.

21. **What are the appropriate roles of collaborators on a Safe-OSE project?**

    Sub-awardee organizations can be included on a Safe-OSE proposal as a way of including personnel with specialized expertise and knowledge pertinent to the success of the project. Consultants (funded or unfunded) may also fulfill similar functions. Collaborators may also assist with testing, red-teaming, documenting, evaluating, and conducting other activities that help the project achieve its goals. The solicitation requests a complete list of collaborators and their roles be included in Other Supplementary Documentation.

22. **If our open-source product has government users, should we seek letters of collaboration from them?**

Yes. Letters from federal, State, and/or local governments and/or Tribal Nations are welcome, but for government users a point of contact with whom NSF can follow up may suffice in lieu of a letter.

23. **Should sub-awardees submit Letters of Collaboration?**

    No. Organizations included as sub-awardees are (or will be) making contractual arrangements with the lead organization for the conduct of specific work on the project – as described in the Project Description, Sub-award Budget, and Sub-award Budget Justification – and therefore do not need to provide other documentation of their commitment and involvement.

24. **Can I sign up as a reviewer for the Safe-OSE program?**

    Yes. To be considered as a potential reviewer, please send an email with your resume to pose@nsf.gov. Please note: You will not be able to serve as a reviewer for proposals received for a particular submission deadline if you are part of a team that has submitted a proposal for the same deadline.

25. **How long will it take for my proposal to be reviewed?**

    NSF staff work to process most submissions within six months of receipt.

26. **Do Letters of Collaboration need to follow the NSF *Proposal & Award Policies & Procedures Guide (PAPPG)* standard format for letters?**

    No. The solicitation indicates that these letters do not have to conform to the standard format specified in the PAPPG. Each letter writer should clearly describe how they have contributed and will continue to contribute to the project. Each letter of collaboration (not to exceed two pages) must include the name of the letter writer, current affiliations (institution or place of employment), and relationship to the members of the proposing team and the project.