Safe - OSE

Safety, Security, and Privacy of Open-Source Ecosystems

U.S. National Science Foundation
Safety, Security, and Privacy of
Open-Source Ecosystems

NSF 24-608: Safety, Security, and Privacy of Open-Source Ecosystems (Safe-OSE)

Welcome!

- Overview presentation (<20 min.)
- Q&A (>30 min.) – **please submit questions via webinar Q&A system (we will not be using the raised hand option or chat)**

https://new.nsf.gov/funding/opportunities/safe-ose-safety-security-privacy-open-source-ecosystems

NSF's Three Strategic Priorities

STRENGTHENING ESTABLISHED NSF

With **investments that expand the frontiers of knowledge and technology**.

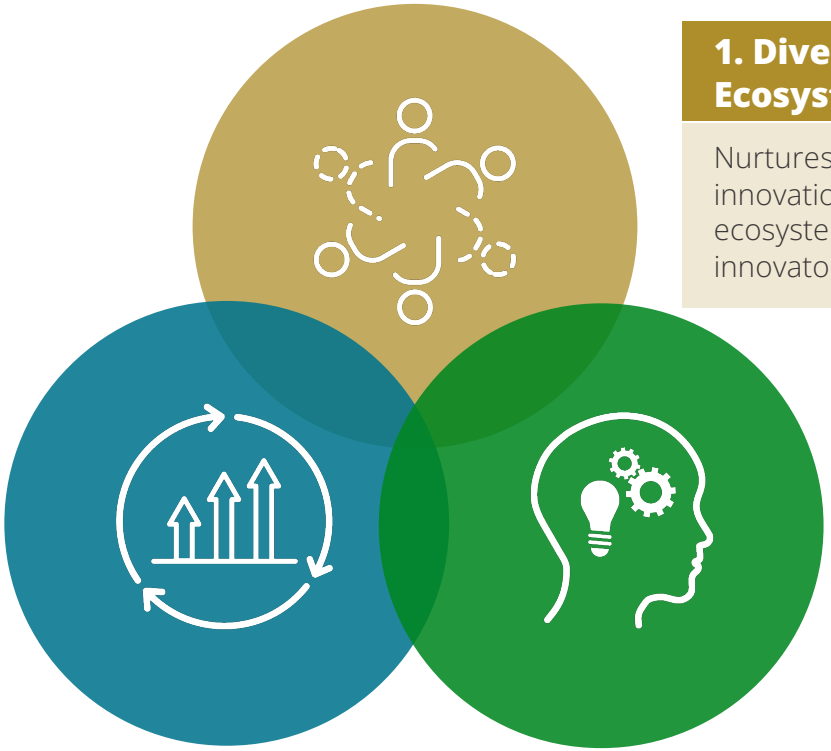
INSPIRING THE MISSING MILLIONS

Using **interventions and capacity building** that enhance and broaden participation.

ACCELERATING TECHNOLOGY AND INNOVATION

Through innovative, **cross-cutting partnerships** and programs.

TIP: Accelerating Research to Impact



1. Diverse Innovation Ecosystems

Nurtures regional and national innovation and technology ecosystems to support researchers and innovators.

2. Technology Translation and Development

Supports researchers, startups, and entrepreneurs to create technologies and innovations with impact.

3. Workforce Development

Supports people from all demographics and geographies to get the training and expertise for the jobs of the future.

POSE and Safe-OSE Program Visions

Technology Translation and Development

Supports researchers, startups, and entrepreneurs to create technologies and innovations with impact.

Diverse Innovation Ecosystems

Nurtures regional and national innovation and technology ecosystems to support researchers and innovators.

POSE: To harness the power of distributed open-source development as an engine of innovation to address challenges of national and societal importance

Safe-OSE: To address significant safety, security, and/or privacy vulnerabilities (both technical and socio-technical) in open-source ecosystems

NOTE: These programs are not limited to **software**-based open-source projects

Safe-OSE Supports Existing, Mature Ecosystems

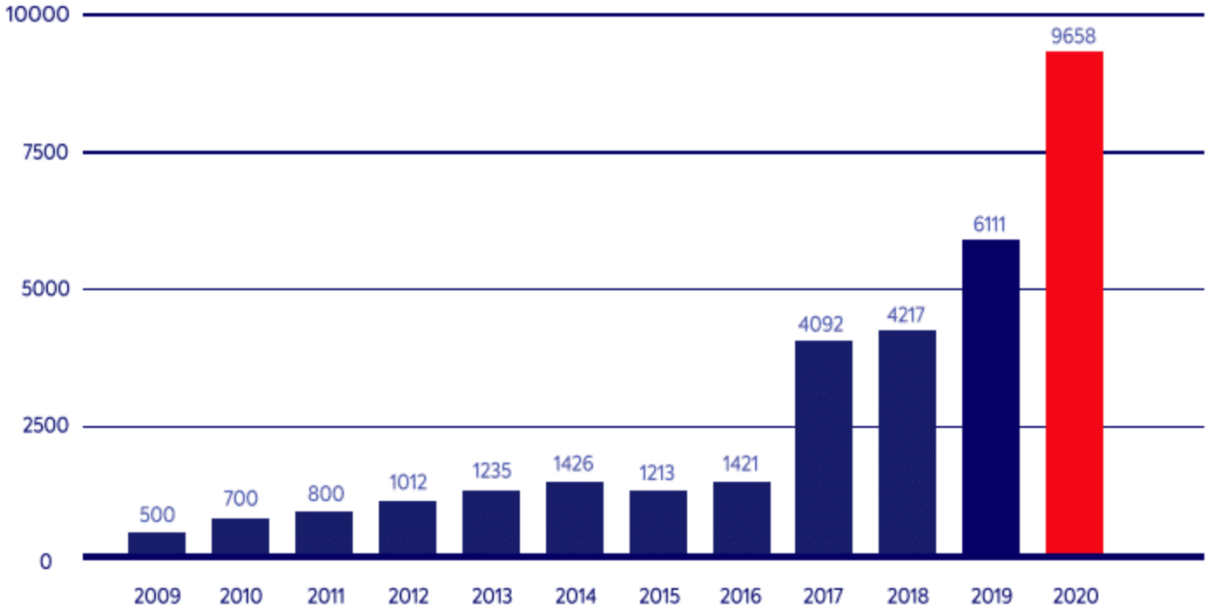
A thriving open-source ecosystem is coordinated via a managing organization that attends to the functions shown at right (and more).

Open-Source Ecosystem/Managing Organization

Existing, well supported open-source products may nonetheless need security, privacy, and safety upgrades to achieve their desired impacts.

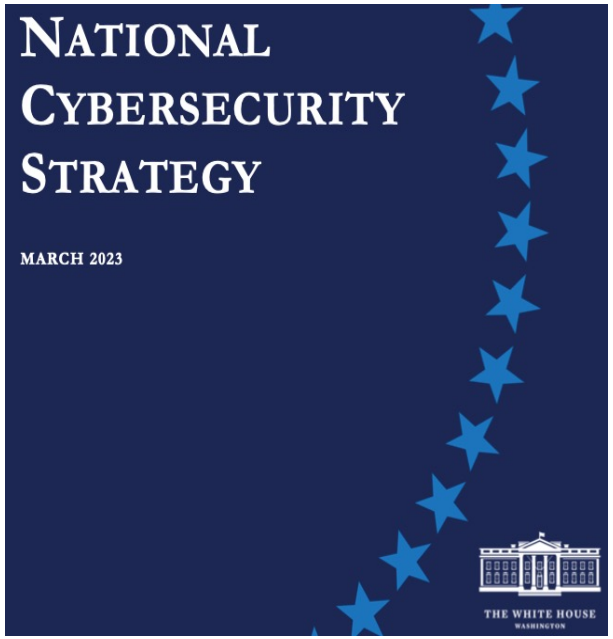
Open Source Vulnerabilities per Year: 2009-2020

Source: Mend.io



Log4j was a remote code execution vulnerability deep inside of an open-source software service maintained by the Apache Foundation. Log4j was discovered in December 2021 and millions of exploits occurred before the flaws were mitigated.

Source: Mend.io

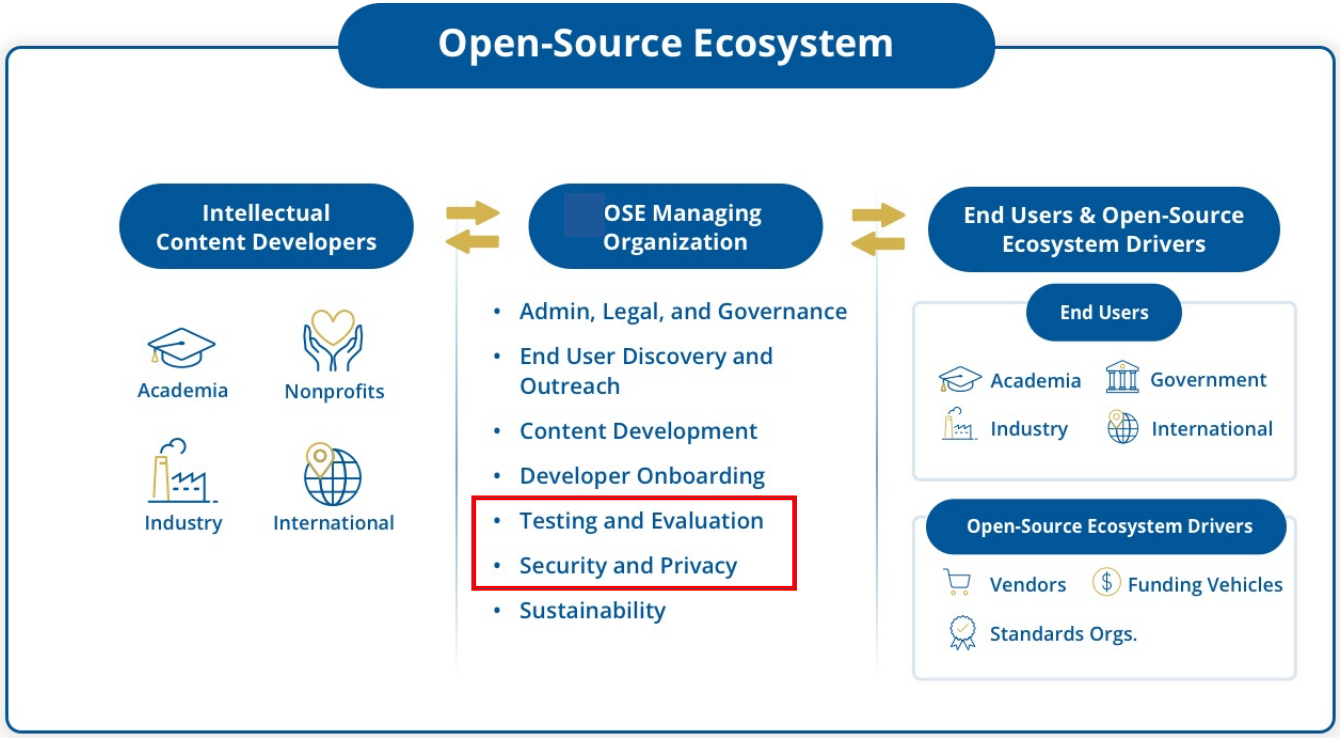


CISA Open Source Software Security Roadmap

Strategic Objective 3.3: the federal government will collaborate with the private sector and OSS community to "**invest in the development of secure software**, including memory-safe languages."

Strategic Objective 4.2: the Federal Government will identify, prioritize, and catalyze the research, development, and demonstration (RD&D) community **to proactively prevent and mitigate cybersecurity risks** in existing and next generation technologies.

What is Safe-OSE Funding For?



Successful OSE-managing organizations facilitate:

1. Product testing and evaluation regimes that help to surface vulnerabilities and flaws at and between releases
2. Practices, methods, features, and designs that prevent attacks, protect privacy, and ensure user and community safety

What is Safe-OSE Funding For: Examples

Core Product	• Adopt/improve static code analysis • Perform memory-safe rewrites • Re-architect vulnerable modules, side-channels
CI/CD	• Improve automated testing • Adopt/improve software composition analysis
Supply Chain	• Implement SBOM • Dependency vulnerability scanning
Sociotechnical	• Developer education, guidance, code review • Risk assessment, rapid response planning • Maintainer vetting, insider threats, social engineering

Successful OSE-managing organizations facilitate:

1. Product testing and evaluation regimes that help to surface vulnerabilities and flaws at and between releases
2. Practices, methods, features, and designs that prevent attacks, protect privacy, and ensure user and community safety

Proposals to Safe-OSE Should…

Provide clear evidence of a thorough understanding of the threat landscape, vulnerabilities, and/or failure modes for the open-source product(s) managed by the OSE.

Situate the OSE's threat landscape in the larger context of known threats and/or vulnerabilities and discuss any significant prior incidents affecting the product(s).

Describe, where appropriate, what other products depend upon the safe, secure, and privacy-preserving functions of the OSE.

Provide a realistic plan for addressing risks related to safety, security, and privacy to address the threat landscape and describe how Safe-OSE funding will meaningfully improve the OSE's capabilities for addressing vulnerabilities as well as for detecting and recovering from incidents.

Be directed at efforts to bolster the OSE's resiliency for recovering from future incidents. Thus, the proposal should articulate how Safe-OSE funding will improve the broader national, societal, and/or economic impacts of the OSE by hardening it against adverse events over the long term.

Not be directed toward fundamental research or at readily resolvable, known bugs/issues, but rather toward strategies, methods, and actions that will fundamentally improve the open-source product's safety, security, and privacy stance.

Safe-OSE Funding: Two Years, $1.5M Maximum

Cooperative Agreement: Year 1

- $500,000 funding for 12 months
- Reverse Site Visit/Reviews in month 11
- NSF decision on second-year funding

Cooperative Agreement: Year 2

- $1,000,000 funding for 12 months
- Final Project Report

Eligibility for Safe-OSE

- Proposals may only be submitted by:
  - US Institutions of Higher Education
  - Non-profit, non-academic US organizations
  - For-profit US organizations
  - Tribal Nations
  - US State and local governments
- Proposing organizations must be U.S.-based, and U.S.-owned and controlled
  - See the solicitation for definitions of "U.S.-based", and "U.S.-owned and controlled"
- Two proposals per organization maximum

Safe-OSE proposals can be multi-organizational, but a single organization must serve as the lead and all other organizations as sub-awardees.

Projects that do not have a managing organization for distributed, ongoing development of a mature open-source product will not be a good fit for the Safe-OSE program.

Who May Serve as PI

- For Institutions of Higher Education:

  - By the submission deadline, any PI, co-PI, or other senior project personnel must hold:
    - a tenured or tenure-track position, or
    - a primary, full-time, paid appointment in a research or teaching position, or
    - a staff leadership role in an Open-Source Program Office or equivalent position

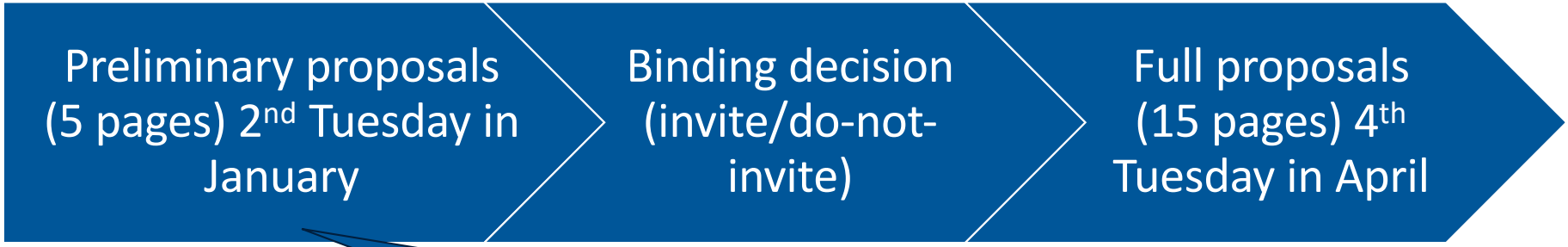
  - Individuals with primary appointments at overseas branch campuses are not eligible. Researchers from foreign academic institutions who contribute expertise to the project may participate but may not receive NSF support.

  - Individuals with appointments at non-US based non-profit or non-US based for-profit organizations are not eligible.

For all other eligible proposing organizations:

The PI must be an employee who is normally resident in the US and must be acting as an employee of the proposing organization while performing PI duties. The PI may perform the PI responsibilities while temporarily out of the US.

Proposal Timeline for Safe-OSE Proposals



Articulate the targeted classes of safety, security, and/or privacy vulnerabilities to be addressed and the broader impacts of addressing them. Discuss, as appropriate, the potential attacks that could take advantage of these vulnerabilities.

Safe-OSE projects must have a publicly available, functional, robust open-source artifact, available under an open-source license, a documented base of users, and a distributed network of developers; the open-source products should have notable, positive societal and/or national impacts.

A previous POSE award is not a prerequisite to apply for Safe-OSE.

Preliminary Proposal Merit Review Criteria

Does the preliminary proposal:

1. Present a convincing case that the targeted OSE addresses **an issue of significant societal or national importance**?
2. Clearly describe the **vulnerability landscape for the OSE** and its product(s)?
3. Provide convincing evidence of a **robust community of developers and that a substantial user base** exists?
4. Present clear **plans for addressing critical vulnerabilities**?

Standard NSF review criteria:
Intellectual Merit: The Intellectual Merit criterion encompasses the potential to advance knowledge; and

Broader Impacts: The Broader Impacts criterion encompasses the potential to benefit society and contribute to the achievement of specific, desired societal outcomes.

Additional Preliminary Proposal Criteria

5. Does the proposing team have the **required expertise and experience** to undertake the activities described in the preliminary proposal?
6. Will **NSF support serve as the critical catalyst** for addressing the identified vulnerabilities (i.e., are there other sources of support that the OSE should be using instead of or in addition to NSF funding)?
7. Does the preliminary proposal **include third-party letters of collaboration** attesting to the importance of the vulnerabilities to be addressed from the perspective of users?

Standard NSF review criteria:
Intellectual Merit: The Intellectual Merit criterion encompasses the potential to advance knowledge; and

Broader Impacts: The Broader Impacts criterion encompasses the potential to benefit society and contribute to the achievement of specific, desired societal outcomes.

Safe-OSE Budget Requirements

- The maximum budget must not exceed $1,500,000, with no more than $500,000 budgeted for the first year of the proposal. Proposals with budgets above these limits will be returned without review.
- Equipment is allowable but must be justified.
- Detailed breakdown and backup documentation for materials, supplied and travel costs required.
- Consultant costs over $1K require backup documentation.
- Subawardees must also provide required documentation.
- Awardees without a NICRA may use a %15 indirect rate.

International collaboration?

International contributors to the ongoing development of an open-source product are welcomed

International collaborators – i.e., organizations that collaborate with a managing organization – are encouraged but cannot be funded via a Safe-OSE award

International subawards or subcontracts cannot be funded via Safe-OSE.

How do I apply?

- Current solicitations:
  - POSE: NSF 24-606
    https://new.nsf.gov/funding/opportunities/pose-pathways-enable-open-source-ecosystems/nsf24-606/solicitation
  - Safe-OSE: NSF 24-608
    https://new.nsf.gov/funding/opportunities/safe-ose-safety-security-privacy-open-source-ecosystems/nsf24-608/solicitation

More questions after today?

Please read the solicitations carefully. Check for updates periodically.

Office hours to answer your questions will be held periodically

Email: pose@nsf.gov

Q&A

Please submit questions via Zoom Q&A

- **Nina Amla (CISE/OAD)**
- **Peter Atherton (TIP/TI)**
- David Liberles (BIO/DEB)
- Parvathi Chundi (TIP/TI)
- Richard Dawes (MPS/CHE)
- Daniel McAdams (ENG/CMMI)
- Deepankar Medhi (CISE/CNS)
- **Daniela Oliveira (CISE/CNS)**
- **Olga Pierrakos (EDU/DUE)**
- Marlon Pierce (CISE/OAC)
- Sylvia J. Spengler (CISE/IIS)
- **Jeffrey Stanton (TIP/TI)**
- **Selcuk Uluagac (CISE/CNS)**
- Teresa Westfall (TIP/OAD)
- Maria Womack (GEO/AGS)

Email for POSE and Safe-OSE Inquiries: pose@nsf.gov

https://new.nsf.gov/funding/initiatives/pathways-enable-open-source-ecosystems
https://new.nsf.gov/funding/opportunities/safe-ose-safety-security-privacy-open-source-ecosystems