

OpenSSF Nov 2024 GB Meeting

Proposed 2025 MVVSR Discussion

Proposed 2025 Roadmap Efforts



Agenda

- Discuss proposed revisions to Mission, Vision, Values, and Strategy (MVVS)
- Review proposed Roadmap
- Discussion



Our road to maturity

In 2024, the Foundation crafted a set of ideals we all desired to work towards

Much effort was spent by the Community, the TAC, and the GB on formalizing a Mission, Vision, Values, and Strategy for the OpenSSF

The TAC has developed a series of slight adjustments to those artifacts as well as following-up to deliver a Roadmap to steer us into the future



[About](#)[Contributors](#)[Technical Initiatives](#)[Training & Guides](#)[Blog & Resources](#)[Events](#)[Join the OpenSSF!](#)

OpenSSF Mission

The Open Source Security Foundation (OpenSSF) seeks to make it easier to sustainably secure the development, maintenance, and consumption of the open source software (OSS) we all depend on. This includes fostering collaboration, establishing best practices, and developing innovative solutions.

OpenSSF Vision

OSS is a digital public good and as an industry, we have an obligation to address the security concerns with the community. We envision a future where OSS is universally trusted, secure, and reliable. This collaborative vision enables individuals and organizations in a global ecosystem to confidently leverage the benefits and meaningfully contribute back to the OSS community.

OpenSSF Values

The OpenSSF serves as a trusted partner to affiliated open source foundations and projects and provides valuable guidance and artifacts, like the top ten Secure Software Development Guiding Principles, to those projects and foundations that encourage security by design and security by default. OpenSSF initiatives should make security easier for open source maintainers and contributors. Consumers of OSS can leverage the output of the OpenSSF to have clear, consistent, and trusted signals to better understand the security profile of OSS content.

The OpenSSF is committed to encouraging all interested stakeholders to participate in the foundation and its technical initiatives (TIs). The OpenSSF is viewed as an influential advocate for mutually-beneficial external efforts and an educator of policy decision makers.

More than just advocacy to Diversity, Equity, and Inclusion (DEI) groups, the OpenSSF remains committed to directly facilitating an environment for all perspectives, all backgrounds, and equitable opportunities for global mentorship and education. The OpenSSF remains committed to continuously evolving these efforts to bring more inclusive and diverse software security education, ensuring stakeholder share opportunities to engage in and receive value from OpenSSF TIs.

OpenSSF Strategy

The OpenSSF strategy is a set of objectives that aim to enhance the security of OSS by developing tooling and processes that make secure development easier, promote a deeper understanding of best practices, and provide support to innovative technical initiatives. The charter is the source of truth for the OpenSSF, and this strategy builds on the charter.

Objectives focus on tooling and processes designed to ensure consistency, integrity, and risk assessment that strengthen the overall security of the OSS ecosystem. This focus supports the community to develop tooling, processes, and educational assets that accelerate OSS security technical initiatives. Accomplishing these objectives will provide maintainers and contributors of OSS (of all skill levels) the ability to proactively or reactively address both existing and emergent security threats.

The OpenSSF strategy is outlined across five key areas:

- **Education and targeted communication:** Develop and promote best practices, guidelines, and educational resources to enhance open source software security awareness and expertise within the ecosystem. OpenSSF advocates with targeted personas (including maintainers, contributors, and consumers) in the OSS ecosystem to improve their default security posture and catalyzes efforts to reduce or eliminate friction in achieving that state.
- **Facilitate collaboration:** Foster a culture of collaboration and inclusion among OSS communities, security experts, and industry stakeholders to sustainably address open source software security challenges effectively with transparent operations and governance.
- **Sustainable technical innovation and enhanced delivery:** Support tooling and process enhancements to existing security capabilities. Deliver new security capabilities to open source ecosystems, such as vulnerability detection, incident response, secure coding practices, and actionable standards.
- **Advocacy and policy:** Advocate for policies and practices that promote OSS security, working with governments, industry bodies, and other relevant organizations.
- **Community engagement:** Actively engage with OSS communities through events, conferences, workshops, and online platforms to foster dialogue, collaboration, and knowledge exchange.

<https://openssf.org/about/>

MVVS

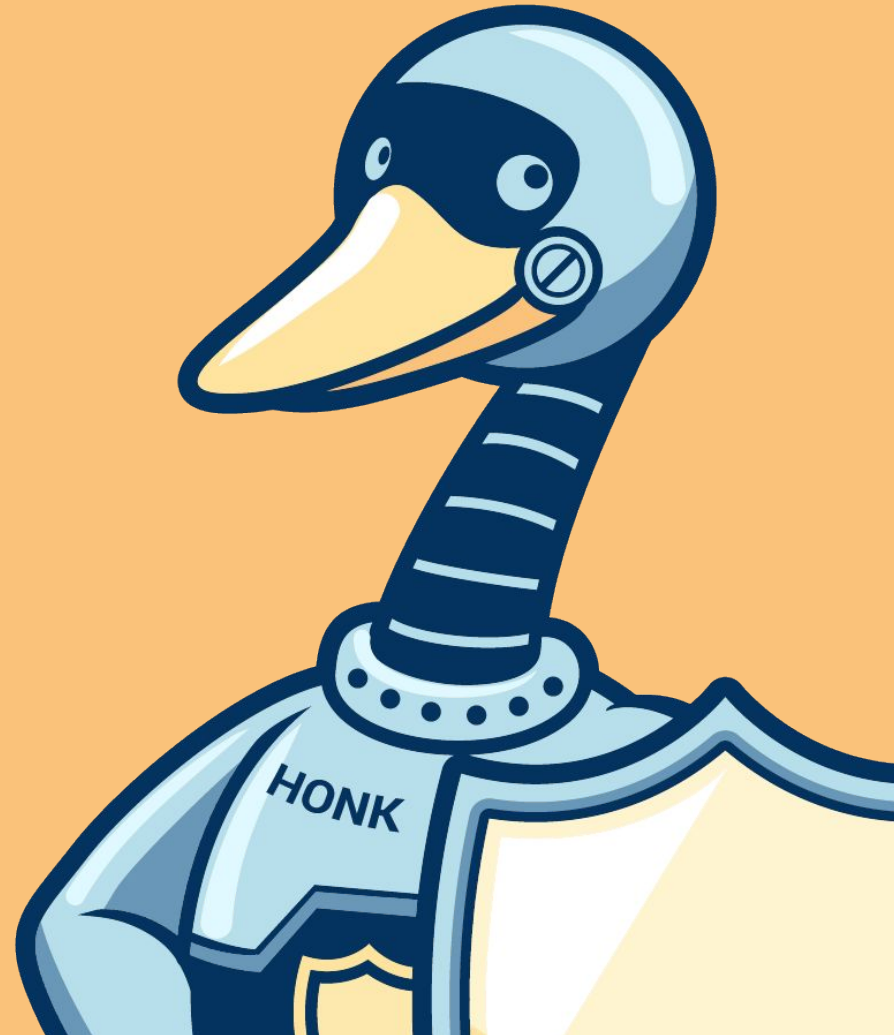
Mission

Vision

Values

Strategy

Full MVSRv3 [text](#)



OpenSSF Mission

The Open Source Security Foundation (OpenSSF) seeks to make it easier to sustainably secure the development, maintenance, *release*, and consumption of the open source software (OSS) we all depend on. This includes fostering collaboration *within and beyond the OpenSSF*, establishing best practices, and developing innovative solutions.



Items in RED are proposed changes from the previously-approved statement

OpenSSF Vision

OSS is a digital public good and as an industry, we have an obligation to address the security concerns with the community. We envision a future where OSS is universally trusted, secure, and reliable. *Producers of OSS (of all skill levels) have the ability to proactively and retroactively address both existing and emergent security threats through low-friction tooling automation, education, and clear and actionable guidance.* This collaborative vision enables individuals and organizations in a global ecosystem to confidently leverage the benefits and meaningfully contribute back to the OSS community.



Items in RED are proposed changes from the previously-approved statement

<https://github.com/ossf/tac/blob/main/technical-vision.md>

OpenSSF Values

The OpenSSF serves as a trusted partner to affiliated open source foundations and projects, and provides valuable guidance and artifacts, ~~like the top ten Secure Software Development Guiding Principles, to those projects and foundations~~ that encourage security-by-design and security-by-default. OpenSSF initiatives should make security easier for open source maintainers and contributors. Consumers of OSS can leverage the output of the OpenSSF to have clear, consistent, and trusted signals to better understand the security profile of OSS content.

The OpenSSF is committed to encouraging all interested stakeholders to participate in the foundation and its technical initiatives (TIs). The OpenSSF is viewed as an influential advocate for mutually-beneficial external efforts and an educator of policy decision makers. More than just advocacy to Diversity, Equity, and Inclusion (DEI) groups, the OpenSSF remains committed to directly facilitating an environment for all perspectives, all backgrounds, and equitable opportunities for global mentorship and education. The OpenSSF remains committed to continuously evolving these efforts to bring more inclusive and diverse software security education; *The OpenSSF will ensure stakeholders have open and transparent opportunities to engage in and receive value from OpenSSF TIs.*

Items in RED are proposed changes from the previously-approved statement



OpenSSF Strategy (summary)

The OpenSSF strategy is a set of objectives that aim to enhance the security of OSS by developing tooling and processes that make secure development easier, promote a deeper understanding of best practices, and provide support to innovative technical initiatives. The [charter](#) is the source of truth for the OpenSSF, and this strategy builds on the charter.

Objectives focus on tooling and processes designed to ensure consistency, integrity, and risk assessment that strengthen the overall security of the OSS ecosystem. This focus supports the community to develop tooling, processes, and educational assets that accelerate OSS security technical initiatives. Accomplishing these objectives will provide maintainers and contributors of OSS (of all skill levels) the ability to proactively or retroactively address both existing and emergent security threats.

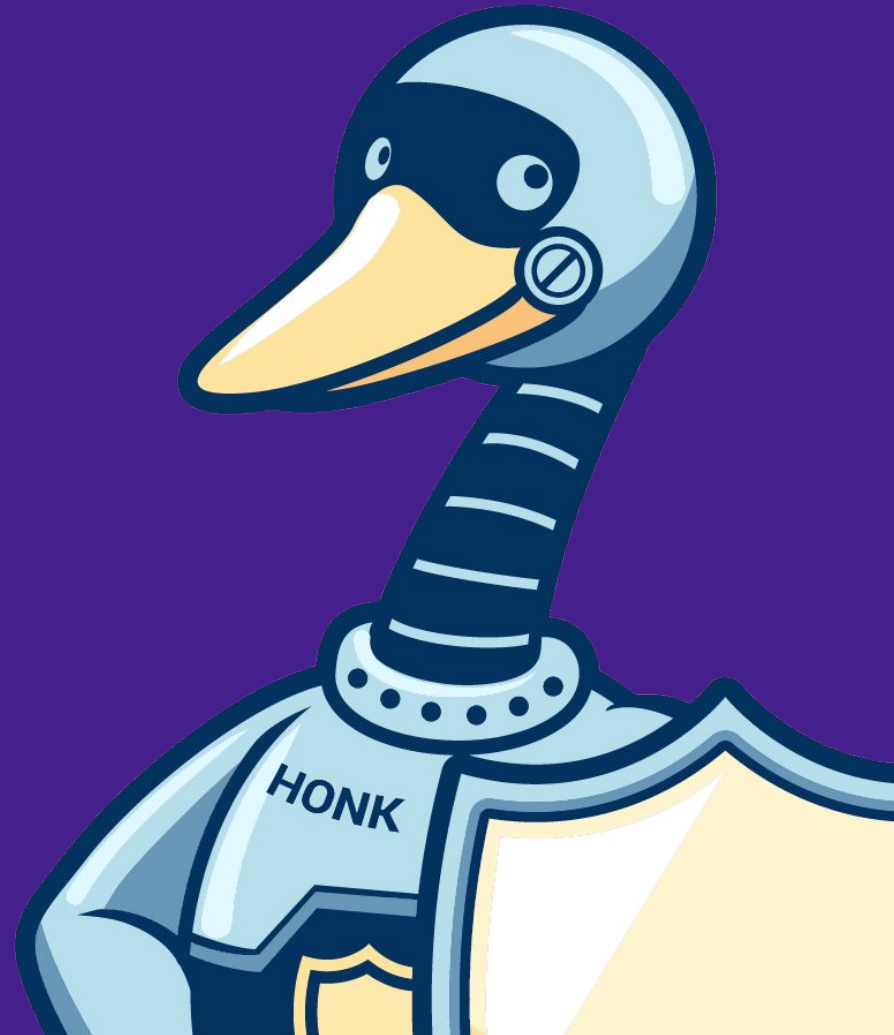
The OpenSSF strategy is outlined across three key areas:

*We will be a **Catalyst for Change**, we will **Educate and Empower the Modern Developer**, and we will **an Ecosystem Leader**.*

Items in RED are proposed changes from the previously-approved statement



R - Roadmap



OpenSSF Roadmap

3 areas of focus for the GB, TAC, and our TIs:

- How do we impact our technological underpinnings to drive adoption of better security outcomes? **Catalyst for Change**
- How do we ensure the evolving security needs of our developer community are being met? **Educate & Empower the Modern Developer**
- How do we interact with others and influence better security? **Ecosystem Leader**

Catalyst for Change

OpenSSF acts as a catalyst for change with producers of OSS to improve “secure by design/default”. Drive technical engagement to create integrated tools that remove barriers to adopting security foundations to improve open source software security.





Catalyst for Change roadmap

- **Finish development of and begin adoption of OpenSSF Security Baseline across LF Foundations**
 - (CNCF, CCC, FinOS) and open source ecosystem (e.g., Python Foundation, OpenJS) providing best practices guides and the ability to start new projects from a more secure default position.
- **Develop an end-to-end architecture for how OpenSSF Technical Initiatives (TIs) and other tools/metadata integrate for both producer and consumer ecosystems.**
 - Resume development and evangelism of the Security Toolbelt, enabling OSS Security tooling conversations through a centralized set of common capabilities and architectural patterns that deliver the desired supply chain security outcomes.
 - Help consumers, producers, and distributors with tooling, reference architectures, and implementations of "secure by design / default" to make it easy for people using, writing and distributing software to make good security decisions.
- **Helping package repositories land security capabilities** through roadmap guidance, implementation guidance, and helping with funding applications and ecosystem implementation proposals.
- **Directly fund TI work that tackles high-impact security gaps and has a defined end date.** When ongoing work is required, help TIs find partners with other organizations, foundations, and open source projects.
 - Prioritize work that eliminates classes of vulnerabilities, and implement secure-by-design tools
- **Apply OpenSSF portfolio for applying DevSecOps to AI/ML/LLM-Ops**, guidance on using AI/ML to improve code security, guidance on using AI/ML for finding and fixing vulnerabilities.
 - Enhance security information available to OSS consumers, focusing on critical projects and create one for the AIML supply chain
 - Connect reference architecture to personas work and include AI/ML engineers and data scientists in OpenSSF. (e.g. There is no "shift security left" in ML engineering. Do our existing tools and integrations support AI/ML use cases?
 - Extending Sigstore signing infrastructure to model cards in AI/ML model signing SIG.)
- **Investigate gaps in developing securely with open source software**
 - Work could include enhancing/creating new linters, IDE tools/plugins, etc to drive earlier adoption of best practices / tooling adoption to allow the developer to make better decisions at the time of writing code; intentionally close gaps.
- **We can measure our Catalyzation success through 2025 Goals such as:**
 - CC1 - Land security capabilities from the Securing Package Repositories Principles into 5+ package repositories
 - CC2 - Create an end-to-end OpenSSF Security Architecture to explain how secure development and software management techniques can be applied throughout the software development lifecycle for all personas
 - CC3 - Coordinate AI/ML/LLM working groups and SMEs to create Applying DevSecOps for AI/ML/LLM development whitepaper

Educate & Empower the Modern Developer

Create and maintain best practices guides & education materials that ensure both current and future OSS developers obtain & maintain sufficient secure development skills. Consumers of OSS can leverage clear, consistent, and easily integrated trusted signals to better understand the security posture of open source content ingested in supply chains.



- **Actively engage with OSS communities through events, conferences, workshops, and online platforms to foster dialogue, collaboration, and knowledge exchange**
 - Be intentional to focus on ecosystems (e.g. conferences to impact repos and their conferences)
 - leverage LF cross-sponsorship opportunities to advocate for improved security
 - Continue to leverage podcast as outlet to showcase members, the community, & security topics of interest. Explore how podcast & similar activities can be leveraged to bring new voices into our community
- **Deliver new security education courses**
 - Deliver Security for Developer Managers course
 - Create Security Architecture course
 - Each TI to craft a <5min explainer video for YouTube & website
 - Partner with LF Education to roll out Global Cybersecurity IT Skills Framework
- **Partner with CNCF to roll out the LF Academic Accreditation program to “certify” collegiate curriculum that meets CNCF/OpenSSF learning objectives**
- **Empower newcomers to meaningfully contribute to OpenSSF TIs**
 - Facilitate OpenSSF TIs to participate in the LFX Mentorship program
- **Ensure our tooling has a product-like experience** that not only delivers a security capability, but is also well documented, easier to use than alternatives, and interoperable with other OpenSSF tooling.
 - Each TI will have training, onboarding materials, ref arches to use, and integration points with other TIs.
- **We can measure our Education and Empowerment success through 2025 Goals such as:**
 - EE1 - Using OpenSSF Security Architecture (CC2) conduct gap assessment to understand missing/deficient tooling/processes as potential areas of funding and collaboration
 - EE2 - Have X educational institutions become part of the Academic Accreditation program
 - EE3 - X TIs will have onboarding documentation and explainer videos

Ecosystem Leader

Be an influential advocate and provide a thought leadership forum for collaboration with partners, OSS communities, security experts, and industry stakeholders on matters important to open source software and supply chain security. Participate meaningfully in standards, frameworks and public policy that impact OSS security. Up-level technical aspects of open source software security when needed to engage with governments, industry bodies, and other relevant organizations.



Ecosystem Leader roadmap

- **Build community and collaborate to influence roadmaps with LF Foundations and similar foundations** and the broader open source ecosystem to improve open source software security
 - Focus on key organizations to collaborate and deliver solution and deepen relationships
 - Participate meaningfully in standards, frameworks and public policy (e.g. SBOM formats, CPE/CVE, AI-ML regulation, etc.).
 - Partner with Foundations and public policy leaders in the development and alignment of the OpenSSF Security Baseline
- **OpenSSF advocates with targeted [personas](#) in the OSS ecosystem** to improve their default security posture and catalyzes efforts to reduce or eliminate friction in achieving that state
 - OSS Maintainer - Developers, developers, developers
 - OSS Supplier - OpenSSF members (and other OSS foundations)
 - OSS Consumer - Downstream enterprise defenders
 - CISO/OSS Regulator - Enterprise security leadership, global governments & regulators/public policy
- **Champion global open source security advocacy and policy.** Engage with global public policy groups on matters impacting/impacted by oss to act as a sounding board/advisor
 - Facilitate global SOSS Policy Summits (DC, EU, Japan) to bring together global OSS security experts and policy makers.
 - Re-energize the Public Policy committee
 - Participate in and contribute OSSF specs to key international standards bodies (i.e., ISO)
 - Influencing the AI/ML Supply Chain regulation and policy with lessons learned from the Software Supply Chain.
 - Conduct an “Harvard Census” style study to identify the top AI/ML OSS Components
- **Document and be inclusive for the maintainer experience**
 - Active our DevRel committee to assist in engaging our developers and community members
- **We can measure our Leadership success through 2025 Goals such as:**
 - EL1 - Adoption of Security Baseline by X Projects in Y LF orgs
 - EL2 - Publish X blog posts/docs related to SOSS/AI at policy regular cadence
 - EL3 - Collaborate with public sector on providing guidance to open source consumers or maintainers through X SOSS Policy Summits that have at least Y attendees, comprised of industry, subject matter experts, and policy makers

Questions



What are the R&Rs for staff?
What do we need from the community?
What do we need from the member orgs?

Thanks!