

Lazy Rivers & Open Source Security

Learn about the OpenSSF with Angelah and Stacey

Angelah Liu, Associate Manager, Marketing & Communications, Linux Foundation

Stacey Potter, Community Manager, OpenSSF



OpenSSF

OPEN SOURCE SECURITY FOUNDATION

ABOUT ME



Stacey Potter

Community Manager, OpenSSF

Stacey brings extensive experience in open source community building, marketing, and event coordination. With a background spanning projects like Minder, Flux and Flagger, OpenFeature, and Keptn, she has played a key role in fostering engagement and driving adoption across cloud-native and open source security ecosystems.



linkedin.com/in/staceypotter/



github.com/staceypotter/



[@staceypotter.bsky.social](https://bsky.social/@staceypotter)



hachyderm.io/@staceypotter

ABOUT ME



Angelah Liu

Associate Manager, Marketing & Communications

Angelah is the Associate Communications & Marketing Manager at the Linux Foundation, supporting marketing initiatives across multiple open source projects, including OpenSSF, the Confidential Computing Consortium, Overture Maps, and AOUSD.

A creative at heart, she thrives on bridging the gap between technical communities and the wider world. Angelah holds a Master of Global Affairs from the University of Toronto, a background that fuels her ability to scale innovation through a lens of international impact. As a dedicated advocate for "Open Source for Good," she uses digital storytelling to ensure open source breakthroughs drive a lasting, positive influence far beyond the tech ecosystem.





OpenSSF

OPEN SOURCE SECURITY FOUNDATION

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)**. This includes fostering collaboration within and beyond the OpenSSF, establishing best practices, and developing innovative solutions.

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.

OpenSSF Working Groups



AI/ML Security



BEAR

Belonging, Empowerment,
Allyship, and Representation



BEST

Best Practices for
Open Source Developers



Global Cyber Policy



ORBIT

Open Resources for
Baselines, Interoperability,
and Tooling



Securing Software Repositories



Supply Chain Integrity



Vulnerability Disclosures

Visit the Working Groups page at <https://openssf.org/community/openssf-working-groups/> for information on each group.

OpenSSF Projects

Best Practices Badge



bomctl



bomctl

gittuf



gittuf

Gemara



GUAC



GUAC

OpenVEX



OpenVEX

RSTUF



RSTUF
REPOSITORY SERVICE FOR TUF

OpenSSF Scorecard



SBOMit



SBOMit

Sigstore



sigstore

SLSA



Zarf



OSPS Baseline



Protobom



Protobom

Minder



minder

OpenBao



Security Insights



Model Signing



Model Signing

OSV Schema



OSV Schema

Fuzz Introspector



Fuzz Introspector

Package Analysis



Package Analysis

Malicious Packages



Malicious Packages

OSS-CRS



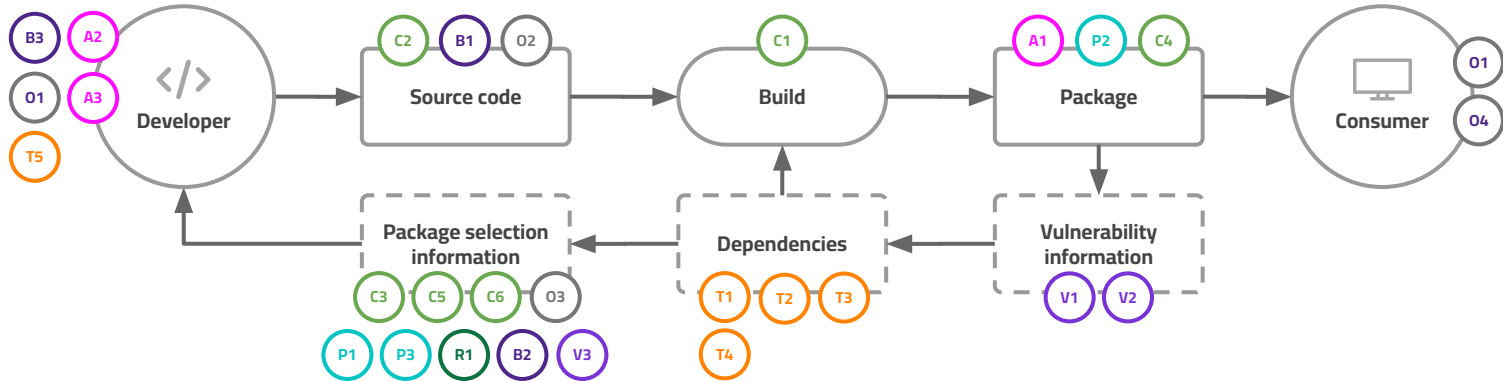
OSS-CRS

Criticality Score



Criticality Score

OpenSSF Projects Landscape



Best Practices

- B1. [OpenSSF Best Practices Badge](#)
- B2. [OpenSSF Scorecard](#)
- B3. [Concise Guides](#)

Securing Software Repositories

- R1. [RSTUE](#)

AI/ML Security

- A1. [Model Signing](#)
- A2. [OSS-CRS](#)
- A3. [Secure Agentic Framework](#)

Global Cyber Policy

Supply Chain Integrity

- C1. [SLSA](#)
- C2. [Gittuf](#)
- C3. [GUAC](#)
- C4. [Zarf](#)
- C5. [Malicious Packages](#)
- C6. [Package Analysis](#)

BEAR (Belonging, Empowerment, Allyship, and Representation)

DevRel Community

Security Tooling

- T1. [SBOMit](#)
- T2. [Protobom](#)
- T3. [bomctl](#)
- T4. [Fuzz Introspector](#)
- T5. [OpenBao](#)

Vulnerability Disclosures

- V1. [OSV Schema](#)
- V2. [OpenVEX](#)
- V3. [Criticality Score](#)

ORBIT (Open Resources for Baselines, Interoperability, and Tooling)

- O1. [OSPS Baseline](#)
- O2. [Minder](#)
- O3. [Security Insights](#)
- O4. [Gemara](#)

Projects

- P1. [Alpha & Omega](#)
- P2. [Sigstore](#)
- P3. [Core Toolchain Infrastructure \(CTI\)](#)

What do you think about when you think of “Security”?

Is it a Dark Art, or something more manageable?



The Lazy River Approach



Find your “lazy river” 👉



Which one are you?

Find your "lazy river" →



FLOAT INTO OPEN SOURCE SECURITY: A SOFTWARE DEVELOPER'S JOURNEY WITH THE OPENSSEF

Learn the fundamentals of secure software development

Just getting started with open source security?

- 1 WRITING SECURE CODE**
 - Secure your development environment
 - Secure your software build and release
- 2 SECURING DEVELOPMENT ENVIRONMENT**
 - Secure your development environment
 - Security baseline toolkits
 - OpenSCAP package review
 - CI/CD
- 3 SECURING BUILD & RELEASE**
 - OpenSCAP toolkits
 - OpenSCAP package review
 - CI/CD
- 4 PROVING BEST PRACTICES**
 - Check you're following security best practice
 - Best practices badge
 - OpenSCAP certification
- 5 CHOOSING SECURE DEPENDENCIES**
 - Choose secure dependencies
- 6 EVALUATING THE OSS YOU USE TODAY**
 - Evaluate your project open source stack
 - OpenSCAP
 - OpenSCAP package review
 - CI/CD
- 7 UNDERSTANDING POLICY & CRA READINESS**
 - Explore how open source connects with government policy and CRA requirements
 - OpenSCAP policy page
 - Free CRA course
 - Baseline
- 8 TECHNICAL GROWTH**
 - Grow your skills and career
 - OpenSCAP training
 - Working groups
- 9 CONTRIBUTING TO UPSTREAM OSS**
 - Contribute upstream
 - OpenSCAP
- 10 SAFE USE OF AI/ML/LLM**
 - Securely explore AI/ML & LLMs
 - AI/ML security WG
 - MLSecOps whitepaper
 - Free AI/ML security course

Developer

FLOAT INTO OPEN SOURCE SECURITY: A SECURITY ENGINEER'S JOURNEY WITH OPENSSEF

Learn the fundamentals of secure software security

Just getting started with open source security?

- 1 SECURITY TOOL LANDSCAPE**
 - Discover and learn about open source security tools for vulnerability scanning, code analysis, and threat detection
 - OpenSCAP
 - OpenSCAP package review
 - CI/CD
- 2 EVALUATION TOOLS**
 - Tools and automation solutions to streamline and scale your open source project assessments
 - OpenSCAP baseline
 - OpenSCAP
 - OpenSCAP
- 3 VULNERABILITY ALERTS**
 - Learn how to monitor and receive timely alerts about vulnerabilities in your open source dependencies
 - OpenSCAP
 - OpenSCAP
 - OpenSCAP
- 4 REGULATORY TOOL MAPPING**
 - Understand how OpenSSF security tools map to regulatory compliance requirements and frameworks
 - Global cyber policy WG
 - OpenSCAP baseline
 - OpenSCAP
- 5 COMMUNITY ENGAGEMENT**
 - Build presence and relationships within open source communities and ecosystems
 - Community calendar
 - Working groups
 - OpenSCAP slack
 - Events
- 6 UPSTREAM COORDINATION**
 - Collaborate with project maintainers on contributions, issues, and project governance
 - Guidance for coordinated vulnerability disclosures
 - Developer relations
 - Contributing guide
 - OpenSCAP
- 7 TECHNICAL GROWTH**
 - Grow your skills and career
 - OpenSCAP training
 - Working groups
- 8 SAFE USE OF AI/ML/LLM**
 - Securely explore AI/ML & LLMs
 - AI/ML security WG
 - MLSecOps whitepaper
 - Free AI/ML security course

Security Engineer

FLOAT INTO OPEN SOURCE SECURITY: AN OPEN SOURCE PROGRAM OFFICE'S JOURNEY WITH OPENSSEF

Learn the fundamentals of open source software security

Just getting started with open source security?

- 1 OSS SECURITY TRAINING**
 - Training resources for your organization to secure software development practice utilizing open source software
 - OpenSCAP
 - OpenSCAP
 - OpenSCAP
- 2 PROJECT EVALUATION METHODS**
 - Methods and frameworks for evaluating the security, health, and maturity of open source projects
 - OpenSCAP
 - OpenSCAP
 - OpenSCAP
- 3 EVALUATION TOOLS**
 - Tools and automation solutions to streamline and scale your open source project assessments
 - OpenSCAP security baseline
 - OpenSCAP
 - OpenSCAP
- 4 UNDERSTANDING POLICY & CRA READINESS**
 - Explore how open source security connects with government policy and CRA requirements
 - OpenSCAP policy page
 - Free CRA course
 - Baseline
- 5 COMMUNITY ENGAGEMENT**
 - Build presence and relationships within open source communities and ecosystems
 - Community calendar
 - Working groups
 - OpenSCAP slack
 - Events
- 6 UPSTREAM COORDINATION**
 - Collaborate with project maintainers on contributions, issues, and project governance
 - Guidance for coordinated vulnerability disclosures
 - Developer relations
 - Contributing guide
 - OpenSCAP
- 7 TECHNICAL GROWTH**
 - Grow your skills and career
 - OpenSCAP training
 - Working groups
- 8 SAFE USE OF AI/ML/LLM**
 - Securely explore AI/ML & LLMs
 - AI/ML security WG
 - MLSecOps whitepaper
 - Free AI/ML security course

OSPO



Checkpoint 1

Entrypoint / Awareness

Pillar: Education & Training

Entrypoint / Awareness – OpenSSF has no single front door

Developer

- “I need to write more secure code”
- On-ramp: LFD121 Developing Secure Software (free course)
- Explore OpenSSF Guides

Security Engineer

- Discover specific tools: GUAC, OpenSSF Scorecard, SLSA
- Trace tool back to OpenSSF ecosystem
- Find the Working Group behind the tool

OSPO

- External pressure: CRA compliance, procurement
- Board-level mandate to audit OSS dependencies
- Governance and policy entrypoints



Software Developer



Security Engineer



OSPO



Software Developer - How to write secure code?

1 **WRITING SECURE CODE**

Want to write secure code?

LFD121 COURSE

BEST GUIDES

FREE

Developing Secure Software
(LFD121)

ENROLL TODAY

THE **LINUX** FOUNDATION Education

OpenSSF Guides

Guides produced by OpenSSF Working Groups to help make open source more secure.

Translation of guides into Japanese.

Secure Coding Guide for Python (pyscg) First Release

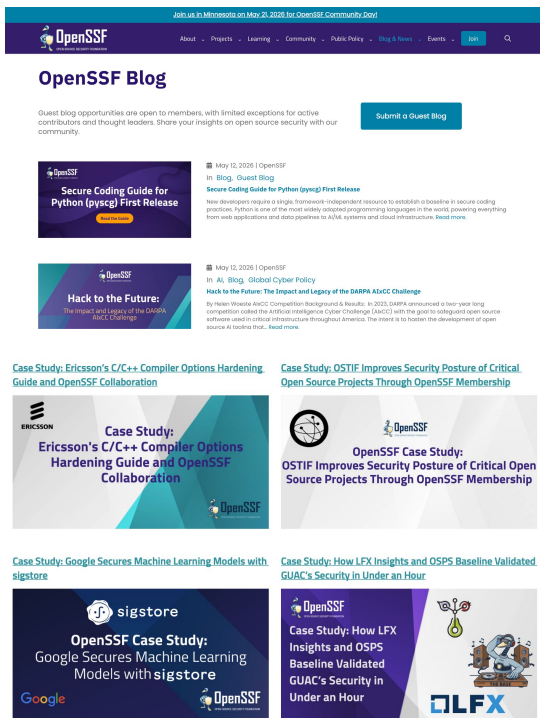
Securing Coding Guide for Python

Improving Risk Management Decisions with SBOM Data

Security-Focused Guide for AI Code Assistant



Security Engineer - How are these tools being built/used?



The screenshot shows the OpenSSF Blog homepage. At the top, there is a navigation bar with links for About, Projects, Learning, Community, Public Policy, Blog & News, Events, and a search icon. Below the navigation bar is the 'OpenSSF Blog' title and a 'Submit a Guest Blog' button. A paragraph of text explains that guest blog opportunities are open to members. Below this are several featured articles:

- Secure Coding Guide for Python (pysec) First Release** (May 12, 2024): A new developer guide to establish a baseline in secure coding practices.
- Hack to the Future: The Impact and Legacy of the DARPA ADGCC Challenge** (May 12, 2024): A retrospective on the DARPA ADGCC Challenge.
- Case Study: Ericsson's C/C++ Compiler Options Hardening Guide and OpenSSF Collaboration**
- Case Study: OSTIF Improves Security Posture of Critical Open Source Projects Through OpenSSF Membership**
- Case Study: Google Secures Machine Learning Models with sigstore**
- Case Study: How LFX Insights and OSPS Baseline Validated GUAC's Security in Under an Hour**



1 SECURITY TOOL LANDSCAPE

Discover and learn about open source security tools for vulnerability scanning, code analysis, and threat detection

CASE STUDIES

TECH TALKS

BLOG

The infographic features a cartoon penguin character holding a sign with a world map and location pins. The background is green and blue with a stylized map outline.



The screenshot shows a YouTube video player for a tech talk. The video title is "How to Use Open Source Project Security Baseline to Better Navigate Standards & Regulations?". The video is from the OpenSSF channel and was published on Thursday, April 24, 2024, at 2 PM ET. The video player interface includes a search bar, a play button, and the OpenSSF logo.



OSPO - What's helpful to my organization?



Cybersecurity Skills Framework



FREE

Developing Secure Software

(LFD121)

ENROLL TODAY



OpenSSF Guides

Guides produced by OpenSSF Working Groups to help make open source more secure.

Translation of guides into Japanese.

- Secure Coding Guide for Python (pyscp) First Release**
- Securing Coding Guide for Python**
This guide is practical, example-driven resource designed to help developers bridge the gap in secure programming for one of the world's most popular languages. It features over 50 rules across nine sections, providing clear "vulnerability vs. mitigator" code examples to help developers build more resilient applications and infrastructure.
- Improving Risk Management Decisions with SBOM Data**
Use this paper to turn SBOM information into clear, repeatable decisions across engineering, security, legal, and operations.
- Security-Focused Guide for AI Code Assistant**



1 OSS SECURITY TRAINING

Training resources for your organization on secure software development practices utilizing open source software

CYBERSECURITY SKILLS FRAMEWORK

FREE COURSES

BEST GUIDES



Checkpoint 2

Activation

Pillar: Community & Contribution

Activation – From passive reader to active participant

Developer

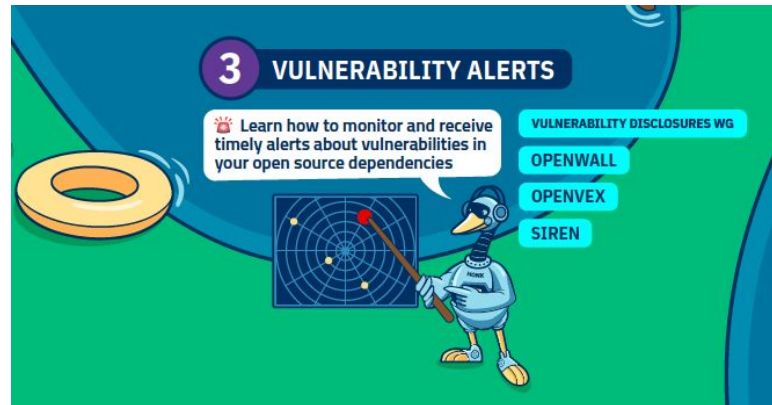
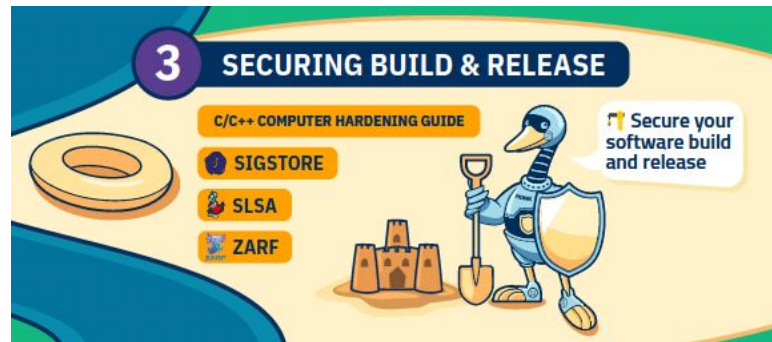
- First upstream security contribution
- Start signing releases with Sigstore
- File a GitHub issue in an OpenSSF repo

Security Engineer

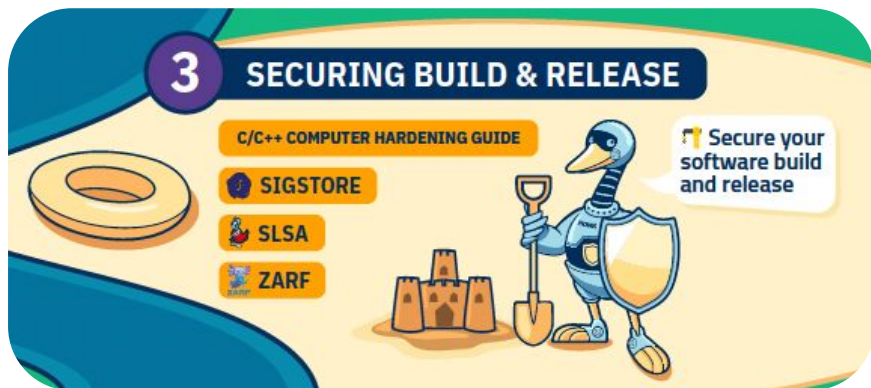
- Attend first Working Group call
- File coordinated vuln disclosure (VulnDisclosures WG)
- Comment on a spec or standard draft

OSPO

- Send someone to a community event
- Adopt the Best Practices Badge internally
- Assign an OpenSSF liaison



Developers – From passive reader to active participant



- First upstream security contribution
- Start signing releases with Sigstore, or self-certify with a Best Practices Badge
- File a GitHub issue in an OpenSSF repo



Security Engineer – From passive reader to active participant

- Attend a Working Group call
- File coordinated vuln disclosure (VulnDisclosures WG)
- Comment on a spec or standard draft



OSPO – From passive reader to active participant

- Send someone to a community event
- Adopt the Best Practices Badge internally
- Assign an OpenSSF liaison

2 PROJECT EVALUATION METHODS



🔍 Methods and frameworks for evaluating the security, health, and maturity of open source projects

CONCISE GUIDE FOR EVALUATING OSS

SECURITY BASELINE TECH TALK

🏆 BEST PRACTICES BADGES



5 COMMUNITY ENGAGEMENT

👋 Build presence and relationships within open source communities and ecosystems.

COMMUNITY CALENDAR

WORKING GROUPS

OPENSFF SLACK

EVENTS



Checkpoint 3

Decision & Consideration

Pillar: Tools, Frameworks, Standards & Policy

Decision & Consideration – Does this actually work for us?

Developer

- Evaluate SLSA, Scorecard & GUAC vs CI/CD pipeline
- Start with OSPS Baseline — not SLSA level 3
- Integrate Scorecard into pull request checks

Security Engineer

- Map OpenSSF tools to CRA, NIST, SOC2 via ORBIT WG
- Use OSPS Baseline as compliance starting point
- Evaluate GUAC for dependency graph visibility

OSPO

- Run Concise Guide for Evaluating OSS on portfolio
- Use Best Practices Badges as a procurement filter
- Identify tools that match your maturity level

6 EVALUATING THE OSS YOU USE TODAY

BASELINE

GUAC

SLSA

Evaluate your current open source stack

← Developer

4 REGULATORY TOOL MAPPING

✓ Understand how OpenSSF security tools map to regulatory compliance requirements and frameworks

GLOBAL CYBER POLICY WG

OSPS BASELINE

ORBIT WG

SecEng →

2 PROJECT EVALUATION METHODS

Methods and frameworks for evaluating the security, health, and maturity of open source projects

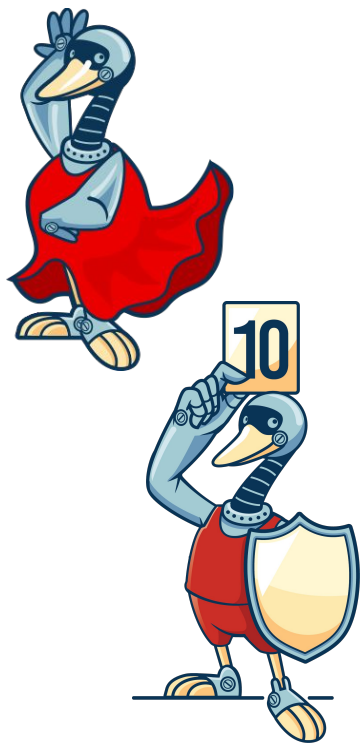
CONCISE GUIDE FOR EVALUATING OSS

SECURITY BASELINE TECH TALK

BEST PRACTICES BADGES


← OSPO


Developer – Does this actually work for us?





- Evaluate SLSA, Scorecard & GUAC vs CI/CD pipeline
- Start with OSPS Baseline — not SLSA level 3
- Integrate Scorecard into pull request checks


EVALUATING THE OSS YOU USE TODAY **6**

 **BASELINE**

 **GUAC**

 **SLSA**

 Evaluate your current open source stack



GUAC



Security Engineer – Does this actually work for us?

Security Engineer

- Map OpenSSF tools to CRA, NIST, SOC2 via ORBIT WG
- Use OSPS Baseline as compliance starting point
- Evaluate GUAC for dependency graph visibility

4 REGULATORY TOOL MAPPING

✓ Understand how OpenSSF security tools map to regulatory compliance requirements and frameworks

GLOBAL CYBER POLICY WG

OSPS BASELINE

ORBIT WG

POLICY DOCK



OSPO – Does this actually work for us?

2 PROJECT EVALUATION METHODS



Methods and frameworks for evaluating the security, health, and maturity of open source projects

CONCISE GUIDE FOR EVALUATING OSS

SECURITY BASELINE TECH TALK

BEST PRACTICES BADGES

3 EVALUATION TOOLS

Tools and automation solutions to streamline and scale your open source project assessments.

OSPS SECURITY BASELINE

GUAC

SLSA



- Run Concise Guide for Evaluating OSS on portfolio
- Use Best Practices Badges as a procurement filter
- Identify tools that match your maturity level



Checkpoint 4

Formal Participation

Pillar: Membership & Governance

Formal Participation – Membership and Governance

Software Developer

7 UNDERSTANDING POLICY & CRA READINESS
Explore how open source security connects with government policy and CRA requirements

- FREE CRA COURSE
- OPENSSEF POLICY PAGE
- BASELINE

9 CONTRIBUTING TO UPSTREAM OSS
Contribute upstream

- JOIN OPENSSEF

POLICY DOCK

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Security Engineer

6 UPSTREAM COORDINATION
Collaborate with project maintainers on contributions, issues, and project governance

- GUIDANCE FOR COORDINATED VULNERABILITY DISCLOSURES
- DEVELOPER RELATIONS
- CONTRIBUTING GUIDE
- JOIN OPENSSEF

4 REGULATORY TOOL MAPPING
Understand how OpenSSF security tools map to regulatory compliance requirements and frameworks

- GLOBAL CYBER POLICY WG
- OSPS BASELINE
- ORBIT WG

POLICY DOCK

OSPO

6 UPSTREAM COORDINATION
Collaborate with project maintainers on contributions, issues, and project governance

- GUIDANCE FOR COORDINATED VULNERABILITY DISCLOSURES
- DEVELOPER RELATIONS
- CONTRIBUTING GUIDE
- JOIN OPENSSEF

4 UNDERSTANDING POLICY & CRA READINESS
Explore how open source security connects with government policy and CRA requirements

- OPENSSEF POLICY PAGE
- FREE CRA COURSE
- BASELINE

POLICY DOCK



Formal Participation – Membership and Governance

Developer

- Become an internal advocate
- Build the business case for membership upward
- Quantify risk reduction from OpenSSF tools

Security Engineer

- Technical champion who presents ROI
- Demonstrate how tools map to regulatory requirements
- Lead your organization's participation within WG

OSPO

- Signs the membership paperwork
- Aligns membership to policy roadmap
- Communicates security leadership to customers

OpenSSF Members



Formal Participation – Membership and Governance

Software Developer

7 UNDERSTANDING POLICY & CRA READINESS
Explore how open source security connects with government policy and CRA requirements

- FREE CRA COURSE
- OPENSSF POLICY PAGE
- BASELINE

9 CONTRIBUTING TO UPSTREAM OSS
Contribute upstream

- JOIN OPENSSF

POLICY DOCK

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Security Engineer

6 UPSTREAM COORDINATION
Collaborate with project maintainers on contributions, issues, and project governance

- GUIDANCE FOR COORDINATED VULNERABILITY DISCLOSURES
- DEVELOPER RELATIONS
- CONTRIBUTING GUIDE
- JOIN OPENSSF

4 REGULATORY TOOL MAPPING
Understand how OpenSSF security tools map to regulatory compliance requirements and frameworks

- GLOBAL CYBER POLICY WG
- OSPS BASELINE
- ORBIT WG

POLICY DOCK

OSPO

6 UPSTREAM COORDINATION
Collaborate with project maintainers on contributions, issues, and project governance

- GUIDANCE FOR COORDINATED VULNERABILITY DISCLOSURES
- DEVELOPER RELATIONS
- CONTRIBUTING GUIDE
- JOIN OPENSSF

4 UNDERSTANDING POLICY & CRA READINESS
Explore how open source security connects with government policy and CRA requirements

- OPENSSF POLICY PAGE
- FREE CRA COURSE
- BASELINE

POLICY DOCK



Checkpoint 5

Advocacy

Pillar: Technical Growth, Upstream Impact

Advocacy – The river doesn't end, the journey deepens

Software Developer 

Developer

- Grow via OpenSSF Training & certifications
- Present at events, become the OSPA Baseline explainer
- Contribute to AI/ML Working Group.

Security Engineer

- Move into WG co-chair roles
- Contribute to MLSecOps whitepaper
- Shape roadmap of tools you leverage

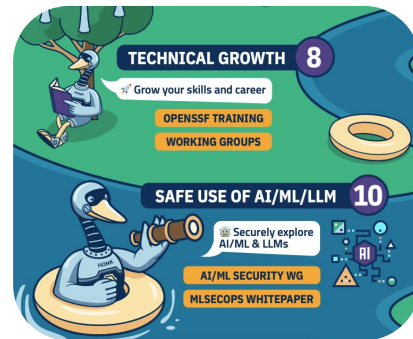
OSPO

- Run internal Best Practices Badge programs
- Contribute to upstream OSS governance
- Sponsor community events and case studies

Security Engineer 



OSPO 



OpenSSF Ambassadors



**MEET THE
OPENSFF
AMBASSADORS**



Ben Cotton



Rob Kenefeck



Ejiro Oghenekome



Justin Cappos



John Kjell



Brandt Keller



Tabatha DiDomenico



Kadi McKean



Roman Zhukov



Katherine Druckman



Hannah Braswell



Wrap-up & CTAs

1. Join **OpenSSF Slack** — lowest barrier, instant community access
2. Explore your **own journey map** — openssf.org/getinvolved
3. **Visit our booth** — Meet the community!
4. **Attend the Global Cyber Policy Working Group Meeting** — **Wednesday, 10-11am in Room 207A**
5. **Join us Thursday** — post-OSS follow-on event for deeper dives
6. Join OpenSSF! **openssf.org/join**

*“You don’t have to know where the river ends to get in the water. **Pick up a tube and start drifting.**”*



OpenSSF Community Day
NORTH AMERICA 2026

May 21, 2026

Minneapolis, Minnesota

#OpenSSFCommunity

View the Agenda & Register Now

Join open source and security
leaders to collaborate on
securing software ecosystems



Ways to Participate



Join a [Working Group/Project](#)



Come to a Meeting (see [Public Calendar](#))



Collaborate on [Slack](#)



Contribute on [GitHub](#)



Become an [Organizational Member](#)



Keep up to date by subscribing to the [OpenSSF Mailing List](#)

Engage with us on social media



X

[@openssf](https://twitter.com/openssf)



LinkedIn

[OpenSSF](https://www.linkedin.com/company/openssf)



Mastodon

social.lfx.dev/@openssf



YouTube

[OpenSSF](https://www.youtube.com/channel/UCv3p0Dk30R118F0X1211111)



Facebook

[OpenSSF](https://www.facebook.com/openssf)

Thank You



Legal Notice

Copyright © [Open Source Security Foundation](#)®, [The Linux Foundation](#)®, & their contributors. The Linux Foundation has registered trademarks and uses trademarks. All other trademarks are those of their respective owners.

Per the [OpenSSF Charter](#), this presentation is released under the Creative Commons Attribution 4.0 International License (CC-BY-4.0), available at <<https://creativecommons.org/licenses/by/4.0/>>. You are free to:

- Share — copy and redistribute the material in any medium or format for any purpose, even commercially.
- Adapt — remix, transform, and build upon the material for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms:

- Attribution — You must give appropriate credit , provide a link to the license, and indicate if changes were made . You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.