OpenSSF Tech Talk

How to Use The Open Source Project Security Baseline to Better Navigate Standards & Regulations

April 24, 2025 | 2PM ET

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Welcome!

- Thank you for joining us today! We will begin at 11:02am PT.
- While we wait for everyone to join, please take a moment to do one (or more) of the following:
  - Please add questions using the Zoom Q&A feature
  - Follow us on X: @openssf, Mastodon: social.lfx.dev/@openssf, LinkedIn: OpenSSF, and Bluesky: @openssf.org
  - Visit our website: https://openssf.org
- This Tech Talk is being recorded
- Slides & recordings will be shared

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Agenda

- Housekeeping
- Speaker Introductions
- Understanding the Challenge
- Learn the OpenSSF Community’s Approach - OSPS Baseline
- Apply the Solution & Get involved!
- Panel Discussion & Audience Q&A
- Important announcements

Help us improve! Tech Talk Survey

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

Antitrust Policy Notice

Linux Foundation meetings **involve participation by industry competitors**, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at **http://www.linuxfoundation.org/antitrust-policy**. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

Code of Conduct

- The Linux Foundation and its project communities are **dedicated to providing a harassment-free experience** for participants at all of our events, whether they are held in person or virtually.
- All event participants, whether they are attending an in-person event or a virtual event, **are expected to behave in accordance with professional standards**, with both this Code of Conduct as well as their respective employer's policies governing appropriate workplace behavior and applicable laws.
- https://openssf.org/community/code-of-conduct/

Q&A

Please submit your questions during the meeting by using the Q&A feature on Zoom.

Thank you!

Introductions

Christopher “CRob” Robinson

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Christopher “CRob” Robinson - Security Lorax, Chief Architect of OpenSSF

Christopher Robinson (aka CRob) is the Chief Security Architect for the Open Source Software Foundation (OpenSSF). With over 25 years of experience in engineering and leadership, he has worked with Fortune 500 companies in industries like finance, healthcare, and manufacturing, and spent six years as Program Architect for Red Hat’s Product Security team.

CRob has spoken at major events such as RSA, BlackHat, and DefCon, and was recognized as a top presenter at Red Hat Summits in 2017 and 2018. He holds certifications like CISSP and CSSLP. He leads several OpenSSF working groups, chairs its Technical Advisory Committee, and contributes to the FIRST PSIRT SIG.

CRob enjoys hats, herding cats, and moonlit beach walks.

Ben Cotton

Ben Cotton is the Open Source Community Lead at Kusari. He is a leader in the GUAC project and Open Source Project Security Baseline SIG Lead. Ben has been active in Fedora and other open source communities for over a decade. His career has taken him through the public and private sector in roles that include desktop support, high-performance computing administration, marketing, and program management. He is the author of *Program Management for Open Source Projects* and has contributed to the book *Human at a Distance*.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Emily Fox

Emily Fox is a DevOps enthusiast, security unicorn, and advocate for Women in Technology. She promotes the cross-pollination of development and security practices. She has worked in security for over 14 years to drive a cultural change where security is unobstructive, natural, and accessible to everyone. Her technical interests include containerization, least privilege, automation, and promoting women in technology. She holds a BS in Information Systems and an MS in cybersecurity.

Megan Knight

Megan is the **Director of Software Communities** at **Arm** where she focuses on upstream engagement with open source projects and ecosystem strategy. She currently serves in a variety of leadership capacities with OpenSSF, Yocto Project, UXL Foundation, and Zephyr Project. In her previous role at Amazon Web Services, she led the IoT and Automotive open source portfolio and served as the Amazon representative on critical dependency open source project boards. She's been kicking it in the open source world for over a decade, driven by people coming together to solve industry-wide problems and the never-ending quest of finding (and sampling) the world's most delicious baked goods.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Understanding the Challenge

Emily Fox
Portfolio Security Architect, Red Hat

From worms to hacks, now breaches and attacks

- Worms and hacks from security research/exploration - discovery of what is possible (CFWAA 1986,Morris worm, Rainbow series, etc.)
- Actioned for malicious execution resulting in data breaches and attacks on critical infrastructure, script kiddies and nation states capitalize on new technology capabilities
- Voluntary approaches due to lack of in-depth understanding and limited expertise.
- Reliant on best practices (which requires discovery, understanding, ability to implement)

Voluntary to Mandatory through regulation

- Businesses:
  - Cybersecurity was “competitive” advantage for reaching exclusive markets (finance, gov)
  - Inconsistent across organizations, consumers still impacted from attacks and breaches
  - “Shoulder to shoulder” public-private partnerships are the core of achieving cybersecurity objectives to ensure synchronized security fundamentals - open source excluded
- Open Source
  - Always voluntary, you get what you see, security through transparent contributions
  - Not in scope of any regulation, “commons”, organizations adopt profusely - transferring requirements onto projects inappropriately
- Increased attacks (frequent & numerous), proliferation of common components (open source won) result in more volume in reported/ discovered vulnerabilities, better understanding/granularity
  - There are more due to more adoption and *awareness of adoption*
- Governments need to protect their citizen consumers - enter regulations

Increasing regulations on software

- We know more now than we did in 2000, ignorance is no longer an excuse
- Common industry agreement and defined need on the basics of security best practices
  - Inconsistent execution, Open Source & AI security concerns
  - OpenSSF Policy Summit 2025 Recap
- Understanding and transparency in what has been done/applied/considered to reduce the vulnerability impact and footprint of software - needed for *informed risk decisions by consumers*
  - Harmonization and supply chain
- Enter CRA… the penultimate combination of cybersecurity requirements reaching beyond the European Union

The OpenSSF Community's Approach: OSPS Baseline

Ben Cotton
Open Source Community Lead, Kusari

What is the Open Source Project Security Baseline?

- A set of security controls for project maintainers…
- …with direct and actionable guidance…
- …across eight categories…
- …in three levels.
- Cross-references to other frameworks (hello, CRA!)

Why OSPS Baseline?

- Original motivation: provide a simple standard for projects
- The excitement? Ease CRA compliance!
  - Or CSF, SSDF, etc
- But also!
  - Improve the overall security posture of the FOSS ecosystem
  - Complimentary to other efforts (OpenSSF Scorecard, Best Practices Badge, etc)

I propose a trade

Manufacturers receive

- Easy way to validate FOSS dependencies for compliance

Maintainers receive

- Easy improvements to security posture
- Zero obligations
- Zero demands for specific changes

OSPS Baseline principles

- **Focused:** no SHOULD, only MUST
- **Realistic:** practical for project maintainers to implement
- **Actionable:** specific guidance on implementing controls
- **Meaningful:** controls should make a real difference

How OSPS Baseline works — levels

1. Code or non-code projects with any number of maintainers or users
2. Code projects with 2+ maintainers and a small number of consistent users
3. Code projects with a large number of consistent users

OR!

1. Sandbox
2. Incubating
3. Graduated

How OSPS Baseline works — categories

- Access Control (AC)
- Build & Release (BR)
- Documentation (DO)
- Governance (GV)
- Legal (LE)
- Quality (QA)
- Security Assessment (SA)
- Vulnerability Management (VM)

How OSPS Baseline works

OSPS-AC-01 - The project's version control system MUST require multi-factor authentication for collaborators modifying the project repository settings or accessing sensitive data.

Reduce the risk of account compromise or insider threats by requiring multi-factor authentication for collaborators modifying the project repository settings or accessing sensitive data.

OSPS-AC-01.01

Requirement: When a user attempts to access a sensitive resource in the project's version control system, the system MUST require the user to complete a multi-factor authentication process.

Recommendation: Enforce multi-factor authentication for the project's version control system, requiring collaborators to provide a second form of authentication when accessing sensitive data or modifying repository settings. Passkeys are acceptable for this control.

- Maturity Level 1
- Maturity Level 2
- Maturity Level 3

External Framework Mappings

- BPB: CC-G-1
- CRA: 1.2d, 1.2e, 1.2f
- SSDF: PO3.2, PS1
- CSF: PR.A-02
- OCRE: 486-813, 124-564, 347-352, 333-858, 152-725, 201-246

How OSPS Baseline works

- Releases versioned by date
- This is a collaborative project: PRs welcome!

How to apply OSPS Baseline to your project

- Evaluate your repository and built assets against the controls
- Declare “this project meets OSPS Baseline level X vYYYY.MM.DD as of <date>!”

...but how?

- Tooling is in the works!
  - darn/darnit: https://github.com/kusari-oss/darn
  - Privateer plugin for GitHub repos: https://github.com/revanite-io/pvtr-github-repo
- Enter the ORBIT Working Group!
  - Brand new
  - Coordinates standards and tooling for security-relevant data

Apply the Solution & Get Involved

Megan Knight
Director of Software Communities, Arm

Next Steps

LEARN

Read more about the OSPS Baseline and dig into the GitHub

1

ADOPT

Adopt the OSPS Baseline across your projects and/or products

2

COLLABORATE

Complaints + compliments discussion on OpenSSF Slack #sig-security-baseline

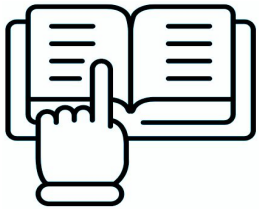
3

CONTRIBUTE

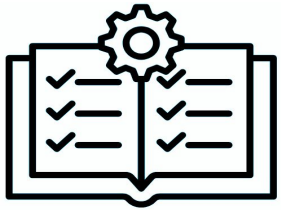
Participate in the Global Cyber Policy and/or Best Practices for OS Developers Working Groups

4

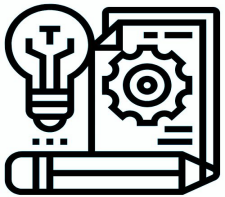
Increasing Awareness with the Global Cyber Policy Working Group



Discussing + Formalizing Cybersecurity **Specifications**



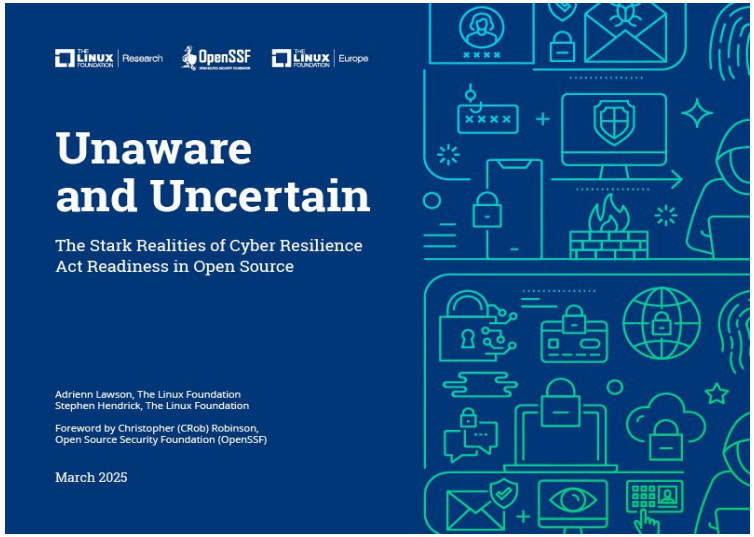
Developing **Tooling**, Processes, and Best Practices for Regulation Compliance



Building **Awareness** + Creating OS Community-Focused Resources

Source: Unaware and Uncertain: CRA Research Report

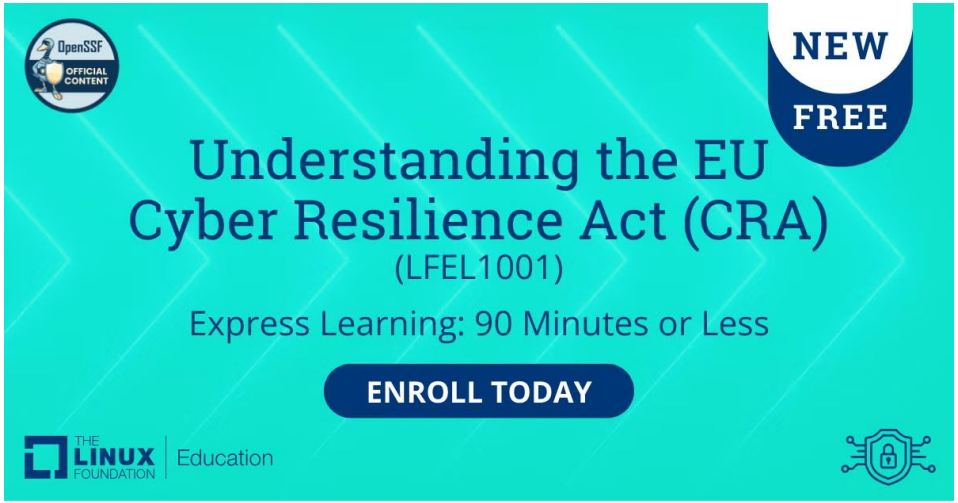
Supporting Research



Download the Report:
https://www.linuxfoundation.org/research/cra-readiness

Download the Report:
https://www.linuxfoundation.org/research/cra-compliance-best-practices

A new (and free!) express learning video course



Key requirements of the EU's Cyber Resilience Act (CRA)

Digital product impacts

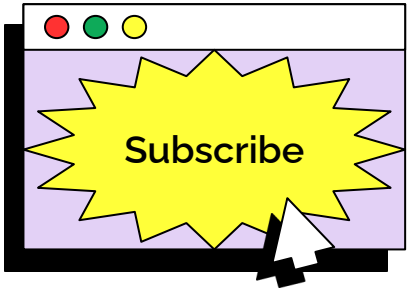
Compliance strategies

How to navigate uncertainties in the law, including for open source software

Global Cyber Policy Work Group

For more information, we encourage you to:

- Visit the WG Repository: Global Cyber Policy WG GitHub
- Join Our Slack Channel: #wg-globalcyberpolicy on Slack
- Subscribe to Mailing Lists:
  - Global Cyber Policy WG Mailing List
  - CRA Readiness+Awareness SIG Mailing List
  - CRA Tooling+Process+Formats SIG Mailing List
  - CRA Spec Standardization SIG Mailing List



Panel Discussion & Audience Q&A

Upcoming Events

OpenSSF Hosted Events:

- Community Day NA: June 26 Colorado Convention Center, Denver, CO
  - Schedule live
  - Sponsor
- Community Day Japan: June 18, Tokyo, Japan.
  - CFP ends this week - April 27
  - Sponsor
- Community Day India: Aug 4 Hyderbad
  - CFP ends this week - April 27
- Community Day Europe: August 28, Amsterdam, Netherlands
  - CFP: Closes May 26
  - Sponsor

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

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

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Engage with us on social media

X
@openssf

LinkedIn
OpenSSF

Mastodon
social.lfx.dev/@openssf

YouTube
OpenSSF

Facebook
OpenSSF

Bluesky
OpenSSF.org

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Subscribe to our mailing list

openssf.org/sign-up

Is your organization a member?

Questions? Contact membership@openssf.org

openssf.org/join

Thank You

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Take our quick Tech Talk Survey

Help us improve!

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Legal Notice