Why you need to care about the CRA

Even if you don’t care about Europe

April 17, 2025 - CMH OWASP
April 29, 2025 - CLE ISC2

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Who is this clown?

CRob - n, adj, and v

Pronunciation: U.S. (K-rowb)

Chief Security Architect, OpenSSF - Linux Foundation

chmod 666 crob.md

43rd level Dungeon Master

26th level Securityologist

Does security stuff on the internet (a series of tubes)

Pirate-enthusiast & hat-owner

FIRST PSIRT SIG leader & VulnCon program committee

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Disclaimer/ Weasel Words

CRob is not a lawyer.

CRob is certainly not YOUR lawyer.

These are thoughts, feelings, and insights from CRob's career; consult YOUR attorney to understand what YOU and YOUR Org

needs to be doing

Created by Microsoft Designer using the prompt "in the style of pixar, show a fun-loving lawyer weasel"

Reading the Room

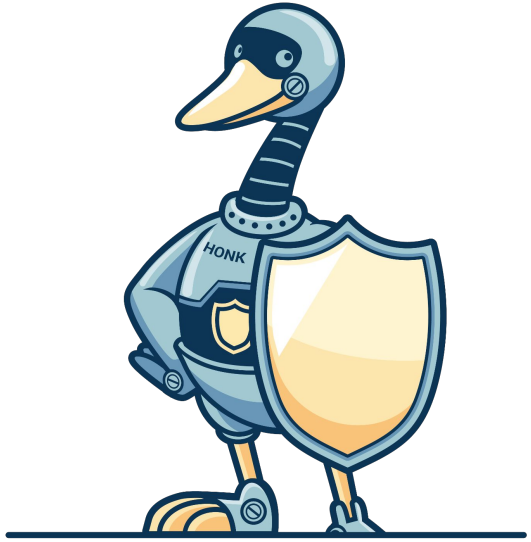
What's your role in software development?

Do you use open source software?

Do you participate in upstream projects?

Do you work for an organization that sells into/has clients in the EU?

Image Source



OpenSSF

OPEN SOURCE SECURITY FOUNDATION

"HONK! HONK, I say! HONK!"

What is the OpenSSF?

What's up with all the Geese?

Mission

Est. 2020

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.

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

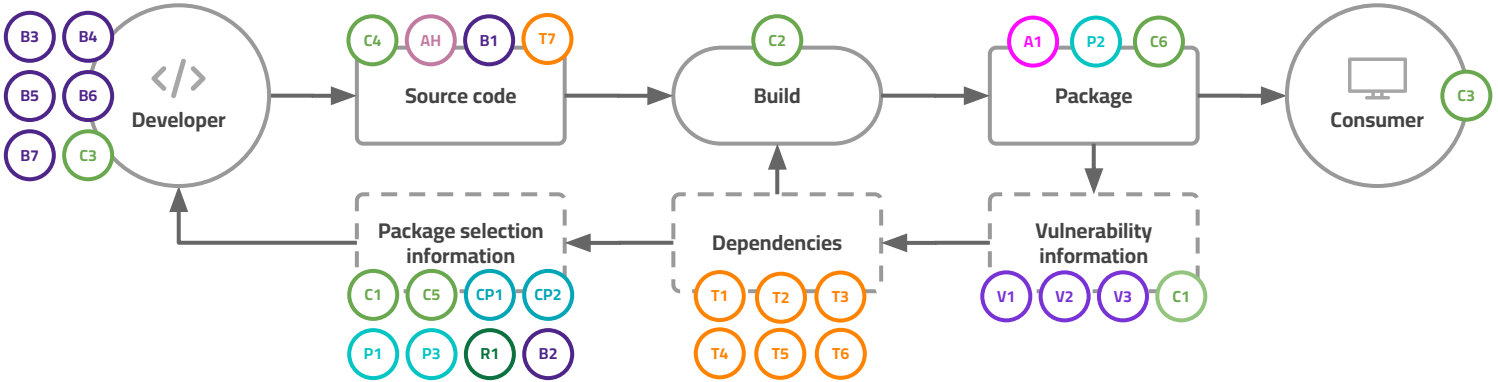
OPEN SOURCE SECURITY FOUNDATION

Assembling a compelling security story

Global cybersecurity legislation is continuing to grow and expand the compliance obligations for enterprises, manufacturers, and impacts upstream open source developers & projects

The OpenSSF has 8 working groups, 19 software projects, and multiple guides, practices, and other artifacts

OpenSSF Technical Initiatives Landscape



Best Practices
- B1. OpenSSF Best Practices Badge project
- B2. OpenSSF Scorecard project
- B3. Education SIG
- B4. Memory Safety SIG
- B5. C/C++ Compiler Options SIG
- B6. Python Hardening SIG
- B7. Security Baseline SIG

DevRel Community

AI/ML Security
- A1. Model Signing SIG

Supply Chain Integrity
- C1. Security Insights project
- C2. SLSA project
- C3. S2C2F project
- C4. Gittuf project
- C5. GUAC project
- C6. Zarf project M

BEAR -Belonging, Empowerment, Allyship, , Acceptance, Representation)

Securing Software Repositories
- R1. RSTUF Project

Security Tooling
- T1. SBOM Everywhere SIG
- T2. OSS Fuzzing SIG
- T3. SBOMit project
- T4. Protobom project
- T5. bomctl project
- T6. Fuzz Introspector project
- T7. Minder project

Vulnerability Disclosures
- V1. CVD Guides SIGs
- V2. OSV Schema project
- V3. OpenVEX SIG

OpenVEX Project

Table Top Exercises (TTX)

Securing Critical Projects
- CP1. criticality_score project
- CP2. Package Analysis project

Projects
- P1. Alpha & Omega project
- P2. Sigstore
- P3. Core Toolchain Infrastructure (CTI)

Global Cyber Policy

www.openssf.org/getinvolved

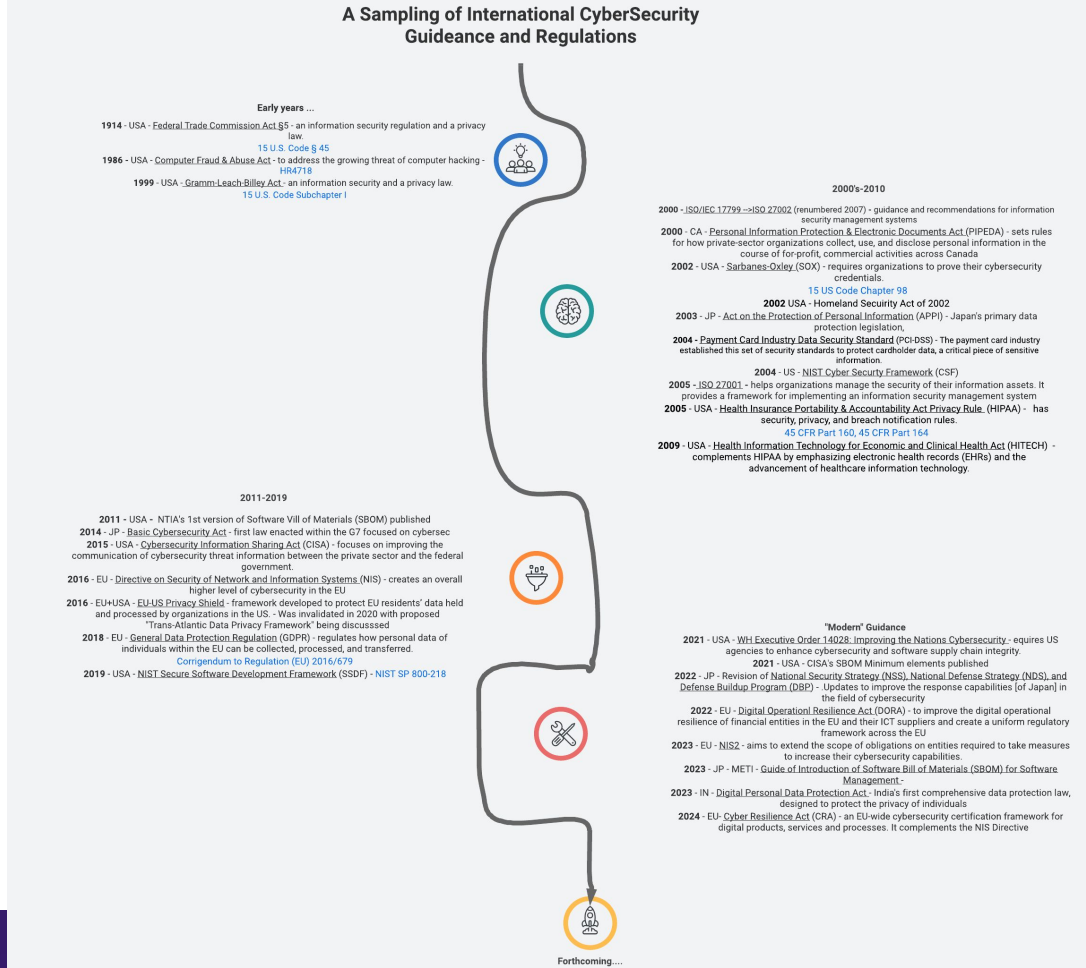
What is this CRA this guy keeps jabbering on about?

Created by Microsoft Designer using the prompt “in the style of pixar an eu cyber threat”

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Welcome to the awesome World of Global CyberSecurity Compliance

Just ~100 years of applicable laws and frameworks that apply to “the cybers”



https://github.com/ossf/wg-globalcyberpolicy/blob/main/documents/2024%20Stewards%20%2B%20Manufacturers%20Workshop/OpenSSF%20CRA%20CyberRegs%20(1).pdf

The EU CRA - Basics and Obligations

The EU Cyber Resilience Act (CRA) establishes essential cybersecurity requirements that all businesses and open source communities operating in the EU will have to implement. As the first EU-wide cybersecurity regulation that explicitly defines the separate roles of manufacturers and open source software stewards, it changes the playing field for the collaborative development of open source software and reshapes the relationship between open source foundations and their member companies. Key topics covered by this presentation include who is responsible for being CRA compliant, what the essential requirements and obligations are, and what support the Linux Foundation will provide in the redefined open source software steward role.

EU Cyber Resilience Act

The EU acts to strengthen the approach to cybersecurity regulation at union level. The CRA aims to achieve 3 policy goals:

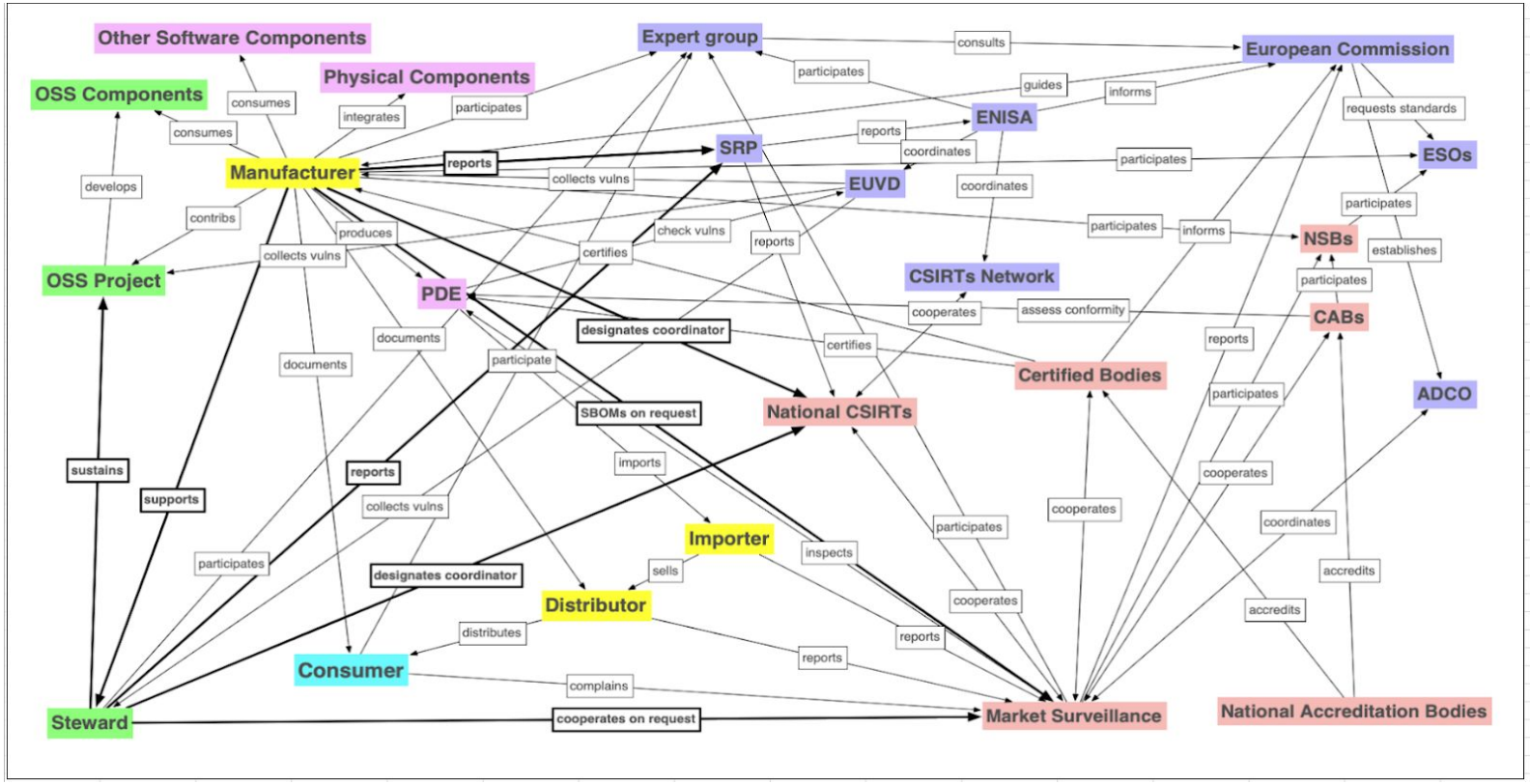
- To reduce vulnerabilities in digital products,
- To ensure cybersecurity is maintained throughout a product's life cycle and
- To enable users to make informed decisions when selecting and operating digital products

The CRA establishes horizontal mandatory cyber-security requirements for all digital products, software and/or hardware.

It imposes objective-oriented and technology-neutral requirements in order to make products available in the EU.

The EU intends to play a leading international role in cybersecurity regulation.

CRA Roles - Nothing confusing about this....



Manufacturers and OSS stewards

Manufacturer:
full range of obligations

...means any natural or legal person who develops or manufactures products with digital elements or has products with digital elements designed, developed or manufactured, and markets them under his or her name or trademark, whether for payment, monetisation or free of charge

(Article 3(18))

Open source software steward:
light-touch regulatory regime

...means any legal person, other than a manufacturer, which has the purpose or objective to systematically provide support on a sustained basis for the development of specific products with digital elements qualifying as free and open-source software that are intended for commercial activities, and ensures the viability of those products

(Article 3(18a))

Annex 1 - the TL/DR of the 90+ page law

Annex I covers ~21 requirements, divided between “cybersecurity” (think SDLC/Sec-By-Design/default + risk management) and “vulnerability handling”

Created by Microsoft Designer using the prompt “In the style of pixar movies, a sloth reads long list of requirements, but it is too long”

https://eur-lex.europa.eu/eli/reg/2024/2847/oj

CRA PSIRT TL/DR from VulnCon 2025 - https://github.com/SecurityCRob/presentations/blob/main/CRA%20PSIRT%20TL_DR.pdf

Meet your (old) new friends - part 1

	Annex I Requirements - “SDLC”
1.1	Appropriate level of cybersecurity based on the risks
1.2a	Made available on the market *without known exploitable vulnerabilities*
1.2b	Made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;
1.2c	*Ensure that vulnerabilities can be addressed through security updates*, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them
1.2d	*Ensure protection from unauthorised access* by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access
1.2e	*Protect the confidentiality of stored, transmitted or otherwise processed data*, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means
1.2f	*Protect the integrity of stored, transmitted or otherwise processed data*, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions
1.2g	*Process only data*, personal or other, *that* are adequate, relevant and limited to what *is necessary in relation to the intended purpose of the product* with digital elements (data minimisation)
1.2h	*Protect the availability of essential and basic functions*, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

Emphasis added

Meet your (old) new friends - part 2

	Annex I Requirements, continued - MOAR SDLC
1.2i	*Minimise the negative impact by the products* themselves or connected devices *on the availability of services provided by other devices or networks*
1.2j	*Be designed, developed and produced to limit attack surfaces*, including external interfaces
1.2k	*Be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques*
1.2l	*Provide security related information* by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user
1.2m	*provide the possibility for users to securely and easily remove on a permanent basis all data and settings* and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner

Meet your (old) new friends - part 3

	Annex I Requirements, continued, continued - CVD/VDP
2.1	*Identify and document vulnerabilities and components contained in products* with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products
2.2	In relation to the risks posed to products with digital elements, *address and remediate vulnerabilities without delay, including by providing security updates*; where technically feasible, new security updates shall be provided separately from functionality updates
2.3	Apply effective and regular tests and reviews of the security of the product with digital elements
2.4	Once a security update has been made available, *share and publicly disclose information about fixed vulnerabilities*, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch
2.5	*Put in place and enforce a policy on coordinated vulnerability disclosure*
2.6	Take measures to *facilitate the sharing of information about potential vulnerabilities in their product* with digital elements as well as in third party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements
2.7	*provide for mechanisms to securely distribute updates for products* with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner
2.8	*Ensure that, where security updates are available to address identified security issues, they are disseminated without delay* and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken

Consequences on non-compliance

Article 64 lays out the framework for Penalties of non-compliance….

***Emphasis** added*

Created by Microsoft Designer using the prompt "in the style of a pixar movie, a cybernetic goose is surprised by a large utility bill"

2. Non-compliance with the **essential cybersecurity requirements** set out in Annex I and the obligations set out in Articles 13 and 14 *shall be subject to administrative fines of up to EUR 15 000 000 or, if the offender is an undertaking, up to 2,5 % of the its total worldwide annual turnover for the preceding financial year, whichever is higher.*

3. Non-compliance with the obligations set out in Articles 18 to 23, Article 28, Article 30(1) to (4), Article 31(1) to (4), Article 32(1), (2) and (3), Article 33(5), and Articles 39, 41, 47, 49 and 53 *shall be subject to administrative fines of up to EUR 10 000 000 or, if the offender is an undertaking, up to 2 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.*

4. **The supply of incorrect, incomplete or misleading information to notified bodies and market surveillance authorities** in reply to a request *shall be subject to administrative fines of up to EUR 5 000 000 or, if the offender is an undertaking, up to 1 % of its total worldwide annual turnover for the preceding financial year, whichever is higher.*

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847#cpt_IV

- Upstream Open Source Developers
- Companies that sell products within the EU
- Companies buying things made in the EU
- Companies that sell or buy things within a country*
- Downstream OSS Consumers
- Disaffected College Students
- Security Enthusiasts
- GRC people/”compliance SUPERfans”!
- People that are just here for the snacks
    - (aka when is this guy going to shut up?)

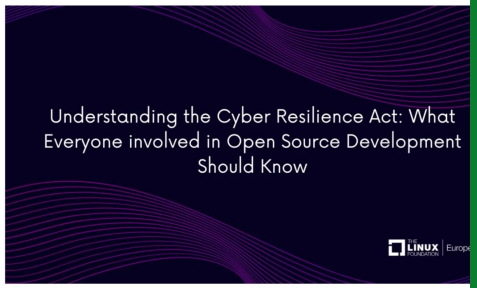
Who should care about this?

20

Ripped from the headlines!

Open Source and the CRA: It Will Not Work

THE LINUX FOUNDATION | 21 SEPTEMBER 2023



Expect to see open source "not approved for the EU" if the EU CRA goes forwar

With the adoption of open source software into the fabric of societies, the ecos
needs to improve how we protect downstream users with regards to cyber sec
OpenSSF is taking that challenge head-on. Many other efforts are underway to
security in open source software critical to the world, starting at the beginning
software supply chain in the projects themselves. The open source ecosystem
at the forefront of software security - not laggards. It's been downstream produ
implementations that generally lack secure software practices. Software provid
devices is often out of sync with the current upstream projects, vendors don't p
software updates, and products are often released to the market with insecure
configurations.

LF Research

Blog

In letter to EU, open source bodies say Cyber Resilience Act could have 'chilling effect' on software development

Paul Sawers — 3:37 AM PDT · April 18, 2023

ELSEVIER

Computer Law & Security Review

Volume 56, April 2025, 106105

The end of open source? Regulating open source under the cyber resilience act and liability directive

Cite

Get rights and content ↗

Open access

ce model leverages collaborative intelligence to drive
fits for both industry and society. As open-source
gly central role in driving the digitalization of society,
nteractions between upstream open-source
anufacturers. They aim to leverage the benefits of OSS,
nts and adaptability across diverse domains, while
countability. The regulatory landscape is on the brink of a major transformation with the recent adoption of both the Cyber Resilience Act (CRA) as well as the Product Liability Directive (PLD), raising concerns that these laws could threaten the future of OSS.

https://www.linuxfoundation.org/blog/open-source-and-the-cra-will-not-work

https://techcrunch.com/2023/04/18/in-letter-to-european-commission-open-source-bodies-say-cyber-resilience-act-could-have-chilling-effect-on-software-development/

https://www.sciencedirect.com/science/article/pii/S0267364924001705

What we want to avoid

Created by Microsoft Designer using the prompt “in the style of a pixar movie an angry mob chase a developer with pitchforks and torches”

Dear Haxx Team Partner,

You are receiving this message because [redacted] uses a product you developed. We request you review and respond within 24 hours of receiving this email. If you are not the right person, please forward this message to the appropriate contact.

As you may already be aware, a newly discovered zero-day vulnerability is currently impacting Java logging library Apache Log4j globally, potentially allowing attackers to gain full control of affected servers.

The security and protection of our customers' confidential information is our top priority. As a key partner in serving our customers, we need to understand your risk and mitigation plans for this vulnerability.

Please respond to the following questions using the template provided below.

1. If you utilize a Java logging library for any of your applications, what Log4j versions are running?
2. Have there been any confirmed security incidents to your company?
3. If yes, what applications, products, services, and associated versions are impacted?
4. Were any [redacted] product and services impacted?
5. Has [redacted] non-public or personal information been affected?
6. If yes, please provide details of affected [redacted] information immediately.
7. What is the timeline (MM/DD/YY) for completing remediation? List the steps, including dates for each.
8. What action is required from [redacted] to complete this remediation?

In an effort to maintain the integrity of this inquiry, we request that you do not share information relating to [redacted] outside of your company and to keep this request to pertinent personnel only.

Thank you in advance for your prompt attention to this inquiry and your partnership!

Sincerely,

[redacted] Information Security

The information contained in this message may be CONFIDENTIAL and is for the intended addressee only. Any unauthorized use, dissemination of the information, or copying of this message is prohibited. If you are not the intended addressee, please notify the sender immediately and delete this message.

https://daniel.haxx.se/blog/2022/01/24/log4-security-inquiry-response-required/

Is anyone DOING anything about this?

Many people are!

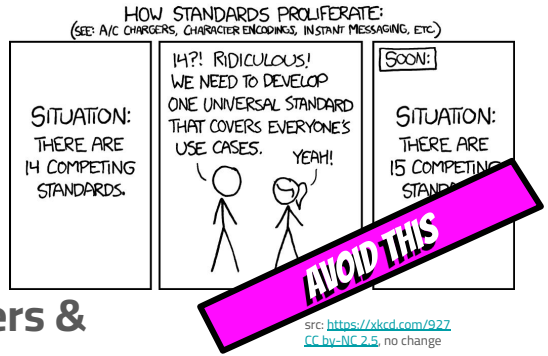
The OSS upstream ecosystem is VERY involved with collaborating with the EC, the assorted expert & standards groups, the projects that they “steward” and the member-manufacturers that must be compliant with the law Dec 2027.

The LF/OpenSSF and the Eclipse Foundation are two of the leading open source expert groups consulting with the myriad of stakeholders affected by this new legislation, but we are not alone.

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

https://tfir.io/openssf-and-lf-europe-collaborate-to-ensure-open-source-compliance-with-laws-like-cra/

Why are we making yet another thing?



1) Global **cybersecurity legislation is continuing to grow and expand** the compliance obligations for enterprises, manufacturers, and **impacts upstream open source developers & projects**
2) **Existing security frameworks** have two primary **assumptions that are not universally true**: you're already in the security space, or you are on GitHub
3) **Continued lack of trust in open source** despite it being transparent, its **difficult to understand how you can trust it**
    a) transparency does not mean all information is available (or exists)
4) Understanding is key, time and again **security is most successful when it meets developers where they are**, in workflow, in jargon, and in **contextualizing effort with cost-benefit analysis**.

Enter the

OPEN SOURCE PROJECT SECURITY (OSPS) BASELINE

<insert dramatic music>
a collab between the OpenSSF, FINOS, CNCF, LF EU & OpenJS

https://openssf.org/projects/osps-baseline/

🗣️ *aa-spuhs bays-line : kindly encouragement and guidance for improving the security of open source projects*

All your Base are belong to us

The OpenSSF Security Baseline was released Feb 2025

Based on a library of well-known cybersecurity frameworks, standards, and global regulations

It includes 40 requirements across 3 levels of maturity covering 8 areas of cyber and application security practices

- Access Control
- Build & Release
- Documentation
- Governance
- Legal
- Quality
- Security Assessment
- Vulnerability Management

https://baseline.openssf.org
https://github.com/ossf/security-baseline

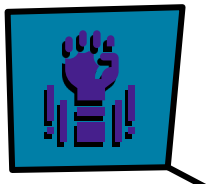
OSPS Baseline principles

- **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

Baseline is grounded in international security frameworks

So **“BASELINING”** helps you be compliant!

Global Frameworks

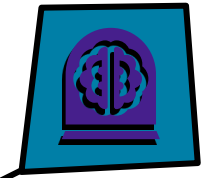


ISO 27001
ISO 27002

International InfoSec frameworks

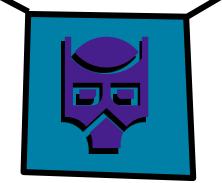
EU CRA + PLD

The Cyber Resilience Act and Product Liability Directive



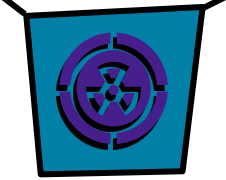
NIST SSDF 1.1

NIST's Secure Software Development Framework



CSA CCM V4

Cloud Security Alliance's Cloud Controls Matrix

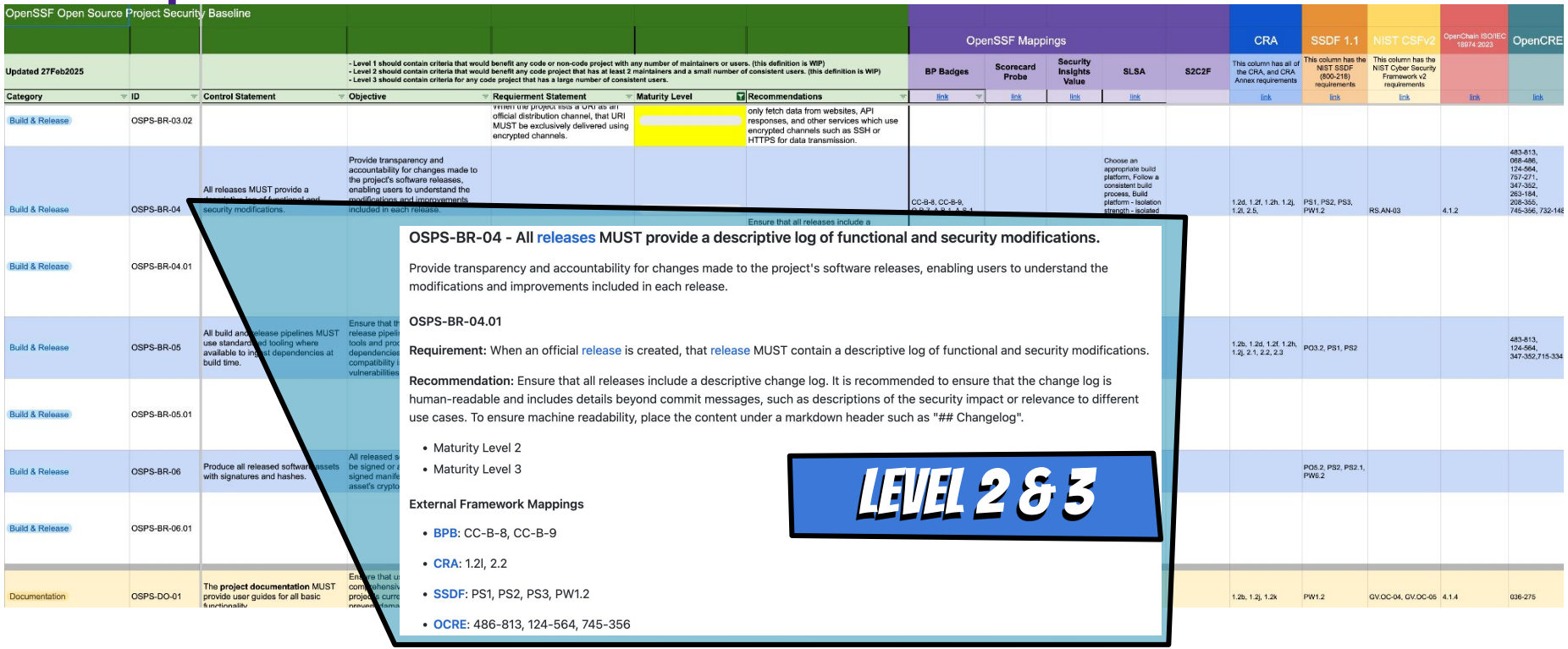


NIST CSF 2.0

NIST's Cybersecurity Framework

...AND MANY OTHERS!

Compliance Crosswalk



https://docs.google.com/spreadsheets/d/1an5mx3rayoz3JRFUepD56zgprpwXBXBG70fVZvIMCpA/

What are these levels you speak of?

- “Universal security floor” for all open source - great for single maintainer or early maturity projects
  - Are you a Foundation? the level 1 baseline should be your first set of criteria for maturing projects (or even accepting projects).
- Let me get my cli, i got this - good for projects with 2 - 6 maintainers and maturing
- Security *flex* - good for highly mature projects that consider security a core competency
  - Are you in a Foundation with project resources? You should strive for this one.

https://baseline.openssf.org
https://github.com/ossf/security-baseline

Why Baseline Matters

Value-prop for Devs

- Gives **direct** and **actionable** advice for improving security practices
- Provides the ability for Developers/projects to show they follow reasonable security measures as well as ways to improve
- **Allow projects to humble-brag** about how great they are
- **Collects common downstream requests** (nags/demands) and advertises them **so Downstream can RTFM** and stop harassing their unpaid Upstream component sources

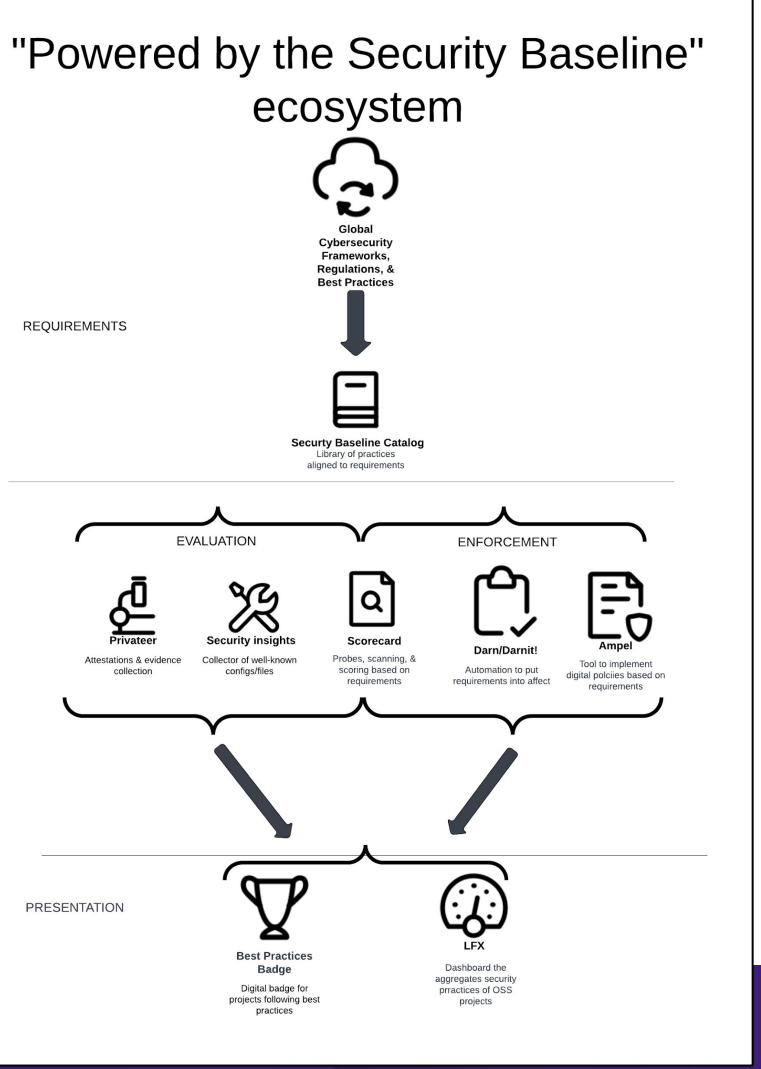
Value-prop for Downstream

- Provides **clear signals** and **evidence/attestations** about upstream component security practices *to allow corporate due-diligence and risk management*
- Provides a **clear checklist** of things that Downstream could go work with (donate/DO) for their Upstream sources
- **Aligns software development practices with global cybersec laws** and frameworks (reduces compliance costs [do once, applicable many])

Future Workflow

- Baseline Catalog v1.0 is ready today!
- Compliance Crosswalk 1.0 ready today!
- Tooling to enable and empower the Baseline Catalog are being developed TODAY!

Follow the ORBIT Working group (Open Resources for Baselines, Interoperability, and Tooling) for more details - https://github.com/ossf/wg-orbit



What's Next for the Baseline?

- Augment Recommendations, templates, and guides
- Add Automation to ease adoption of the Baseline Criteria
- Develop Evidence and Attestation collection/publication so downstream can leverage upstream artifacts for their own compliance needs
- Integrate into LFX for "single pane of glass" holistic view
- Define Reference Architecture that shows end-to-end view of Baseline & other components

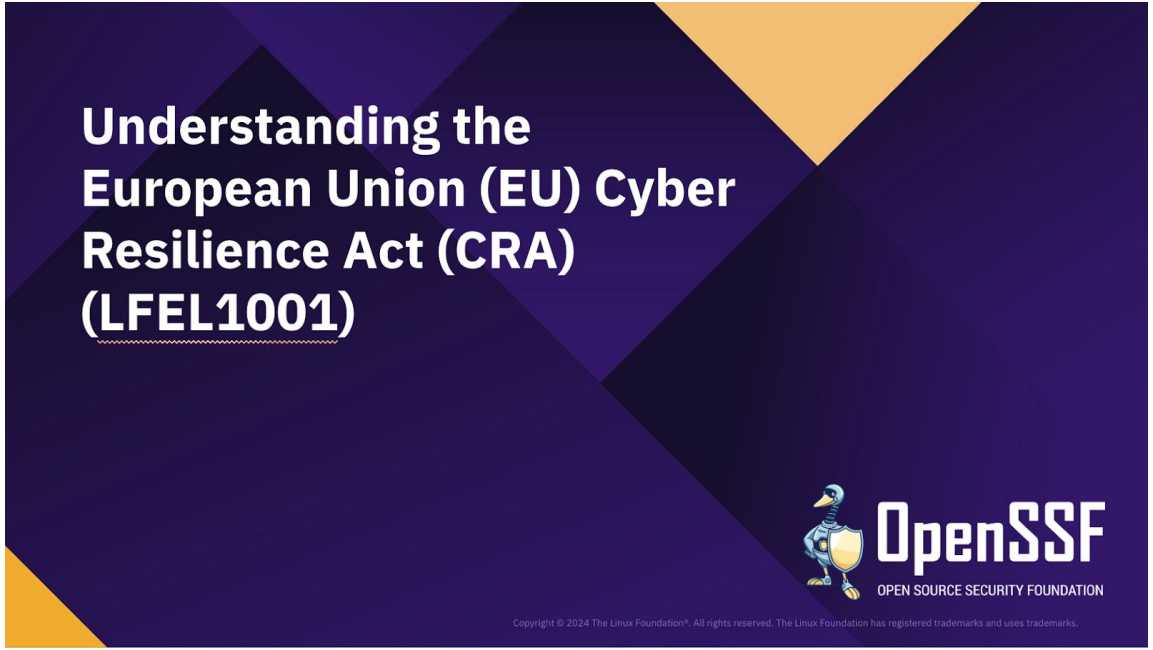
OpenSSF
OPEN SOURCE SECURITY FOUNDATION

“CRA 101”

One of the 1st deliverables of the CRA Awareness SIG will be a free educational course covering the CRA

Available starting 16April2025

Additional courses are planned, including how to conduct Risk Assessments throughout the development and productization lifecycle



https://training.linuxfoundation.org/express-learning/understanding-the-eu-cyber-resilience-act-cra-lfel1001/

How you can help!

Feedback

Take a look and let us know what isn't clear

Contribute

Submit your suggested changes, contribute automation and tooling

Implement

Adopt it for your project or projects in your Foundation

Where to learn more/get engaged

The CRAfish ⇒ 

EU CRA portal - https://www.european-cyber-resilience-act.com/

EU Expert Group - https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3967

ENISA – https://www.enisa.europa.eu/search?keys=cra#contentList

BSI (proactive National CERT, lots of useful implementation guides) – https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber_Resilience_Act/cyber_resilience_act_node.html

OpenSSF Global Cybersecurity Policy Working Group - Open, public forum where anyone can attend and participate https://github.com/ossf/wg-globalcyberpolicy/tree/main

OpenSSF Public Policy website + CRA microsite + other resources – https://openssf.org/?s=cra

LF Research “Unaware and Uncertain - The Stark Realities of Cyber Resilience Act Readiness in Open Source” - https://www.linuxfoundation.org/research/cra-readiness?hsLang=en

Eclipse ORC Working Group – https://orcwg.org/

Thank You

@~~SecurityCRob~~

@SecurityCRob@infosec.exchange

https://github.com/SecurityCRob

The Security Unhappy Hour,
Chips & Salsa
What's in the SOSS?

https://www.linkedin.com/in/darthcrob/

OpenSSF
OPEN SOURCE SECURITY FOUNDATION

Legal Notice