OpenSSL CONFERENCE

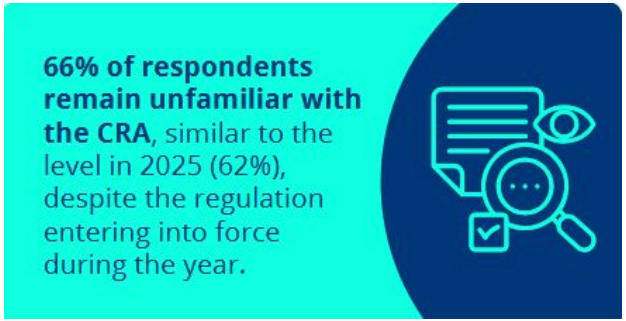
The EU CRA vs. Community

Jaroslav Reznik, Red Hat
Roman Zhukov, Red Hat

§ PRIVACY AS A FUNDAMENTAL HUMAN RIGHT

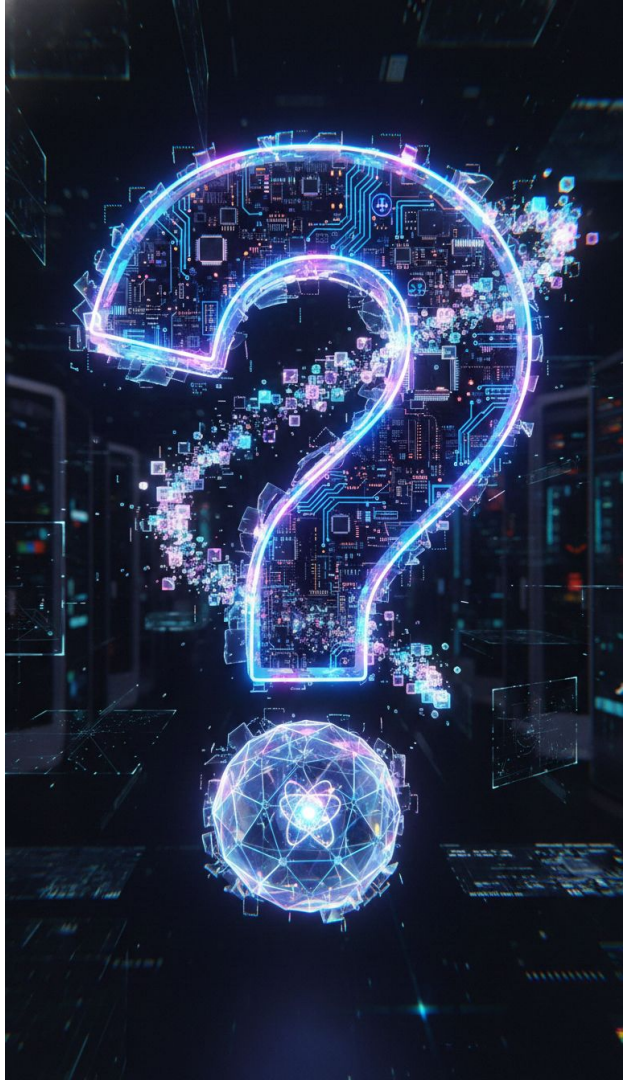


1 Have you heard about the EU CRA?



2 Do you think you or your projects have some CRA obligations?

3 Do you want your project to be at a good quality widely adopted and widely adopted by users?



To safeguard European consumers of Products with Digital Elements (PDE)

Cyber Resilience Act (CRA) establishes essential cybersecurity requirements for companies operate in the EU.

Core Goals

- Reduce vulnerabilities
- Product lifecycle security
- Enable Informed decisions for users

Scope & Roles

- Targets mostly Manufacturers (vendors), Importers and Distributors
- Covers 3rd party dependencies
- Defines open source Stewards

Compliance

- Worldwide applicability for commercial activity within EU
- Fines up to €15M or 2.5% global turnover

September 2026
Vulnerability Reporting Obligations

December 2027
Full Force Implementation

PDEs are...



src: https://knowyourmeme.com/memes/x-x-everywhere

- Consumer devices, toys
- Simple IoT device

90%+ of SW and HW

Default Category

- Smart home
- Operating Systems
- Web browsers
- Password mgrs.

Important Class I (19)

- Firewalls
- Tamper-resistant CPUs
- Hypervisors and CRS

Important Class II (4)

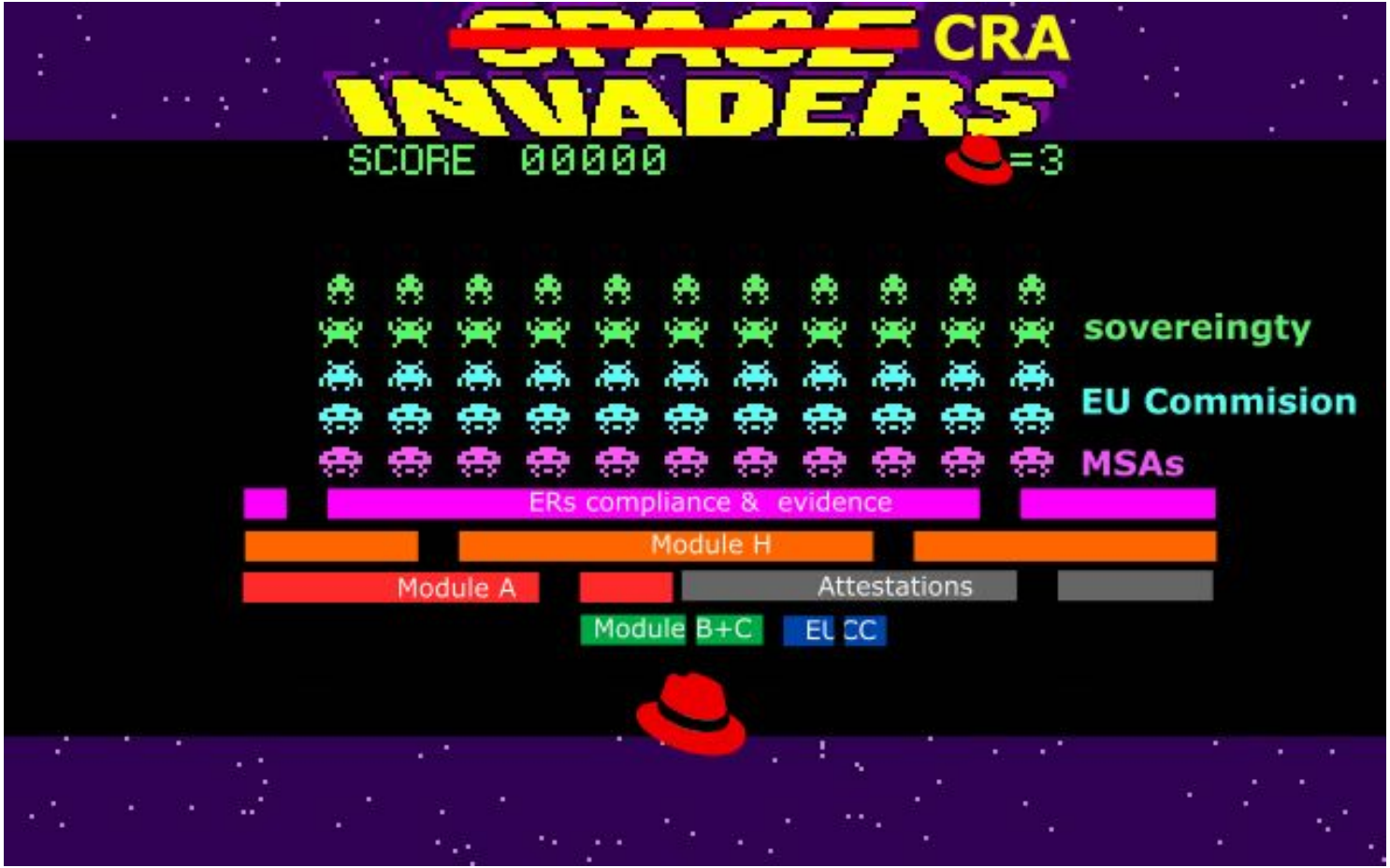
- HW Devices w/Security Boxes
- Smart meter gateways

Critical (3)

?

Source code, binary, container – all counts. And YES! It all can be open source!

Compliance layers



Out of Scope

- Own use of products
- Unfinished SW or not a product (alfa, beta, research, docs)
- Products covered by other regulations or directives, incl. automotive, medical, aviation, national security
- SaaS – if not designed solely for normal functionality of a PDE
  - If the cloud part goes down, and the product breaks – that cloud part is in scope as Remote Data Processing Solutions (**RDPS**).
- **Free and Open Source SW** (FOSS) - if not placed on the EU market (used in course of commercial activity).



Official CRA guide and FAQ by the EU Commission:
https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

public inbox for libc-alpha@sourceware.org

search help / color / mirror / Atom feed

* Cybersecurity Risk Assessment Request from Emerson for libnsl
@ 2025-08-11 11:37 [redacted] [EMR/MSOL/PUNE]
2025-08-11 21:57 ` [redacted]
0 siblings, 1 reply; 3+ messages in thread
From: [redacted] [EMR/MSOL/PUNE] @ 2025-08-11 11:37 UTC (permalink / raw)
To: bug-libc
Cc: [redacted] [EMR/MSOL/PUN
[redacted] [EMR/MSOL/PUNE], [redacted]

[-- Attachment #1: Type: text/plain, Size

Hello,

I hope this message finds you well.

Sr. No.

Queries to Vendor

Response from Vendor (Yes/No)

Additional Remarks from Vendor

1

Is Secure Software Development Lifecycle followed for developing this component?

8

Do you comply with EU-CRA requirements?

9

Do you provide proof of conformity regarding adherence to EU-CRA? If yes please mention details in Remark column



public inbox for libc-alpha@sourceware.org

search help / color / mirror / Atom feed

* Cybersecurity Risk Assessment Request from [redacted] for libnsl
@ 2025-08-11 11:37 [redacted] [EMR/MSOL/PUNE]
  2025-08-11 21:57 ` Mark Wielaard
  0 siblings, 1 reply; 3+ messages in thread
From: [redacted] [EMR/MSOL/PUNE] @ 2025-08-11 11:37 UTC (permalink / raw)
  To: bug-libc
  Cc: [redacted]

[-- Attachment #1: Type: text/plain, Size: 2539 bytes --]

Hello,

I hope this message finds you well.

As part of our ongoing efforts to comply with the EU Cyber Resilience Act (CRA), we are currently conducting a cybersecurity risk assessment

To support this initiative, we kindly request your input on the following questions related to your software product "libnsl" with version 2.

Additional Information:

  *   Purpose: This security assessment is part of our due diligence and regulatory compliance obligations under the EU CRA.
  *   Confidentiality: All information shared will be treated as confidential and used solely for the purpose of this assessment.
  *   Contact: Should you have any questions or need further clarification, please feel free to reach out by replying directly to this email.

We kindly request your response by Monday, August 25, 2025, to ensure timely completion of our assessment process. Thank you for your cooperat

Thanks for giving us exactly 2 weeks, bro =)





> Open Source
> Maintainers
> owe you nothing.
>
> Mike McQuaid

https://mikemcquaid.com/open-source-maintainers-owe-you-nothing/

Important Roles in CRA

Manufacturer - natural or legal person who develops PDEs = **vendor**.

Most obligations, full liability and penalties.

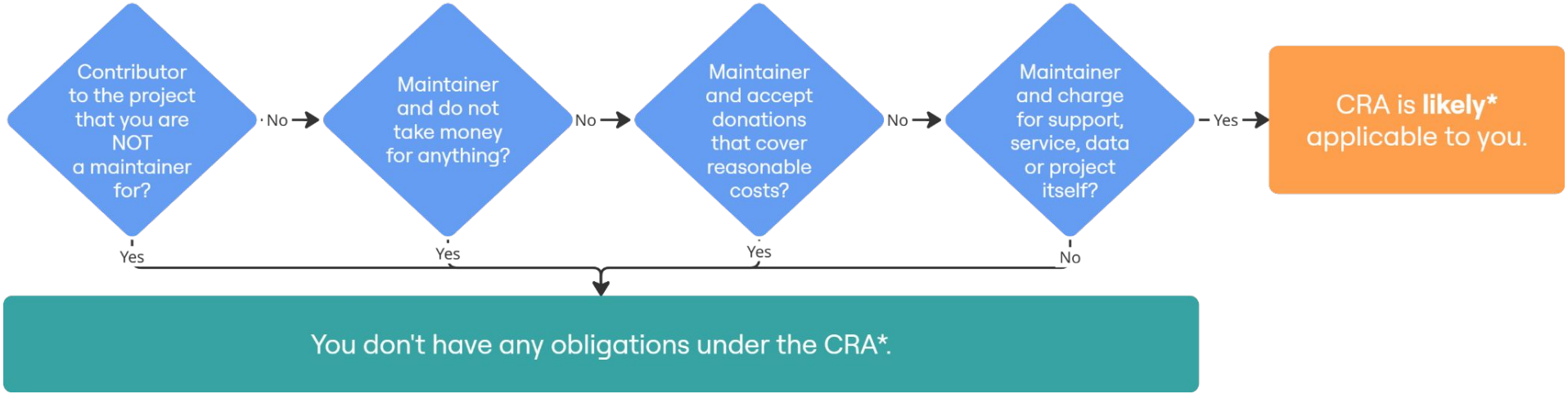
Importer and **Distributor** - bringing a product into the EU market (re-sells PDEs) = **partner**.

Developer, **Contributor** and **Maintainer** of Open Source - **out of scope** if don't monetize project.

OS SW **Steward** - provides sustained supports for a FOSS project (not product), e.g. a foundation or big company.

Most FOSS projects will not have a Steward :(





* Most likely. EU CRA is actively evolving regulation. Not a legal advice.

✅ Non-commercial -> Not a Manufacturer

- Developing FOSS without monetisation
- Receiving donations that cover actual costs
- Being employed to contribute code to a FOSS project
- Publishing on public repositories (contributor)
- Paid support for the PDE you don't build (not a manufacturer)

⚠️ Commercial activity indicators -> Manufacturer

- Charging a price for the software
- Monetising via a platform built around it
- Requiring personal data processing beyond security needs
- Donations exceeding costs of development and living
- Charging for security updates



- Am I subject to the CRA if I earn a living from the open source project I maintain?
- Can a solo maintainer be considered as an open-source software Steward?
- Does the popularity of my open source project expose me to CRA regulation or to a Steward?
- How can I clear communicate I am NOT subject to the CRA to downstream users?
- What additional obligation would I have if I had a Steward?

More at:

cra.orcwg.org/faq/

Why Red Hat Cares

Red Hat as a Manufacturer

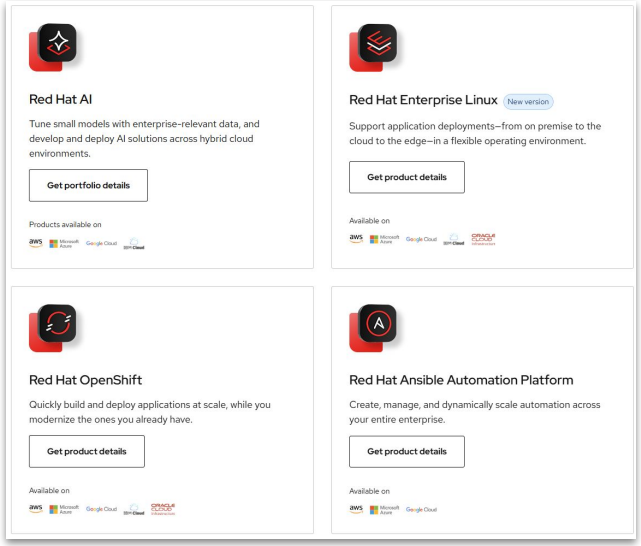
- Provider of enterprise open-source software solutions for the global market, including the EU.

Red Hat as a potential Open Source Software Steward

- Red Hat's relationship with open source software is foundational. The company actively supports Fedora and countless others projects.

Red Hatters are Contributors and Maintainers

- Thousands of Red Hatters contribute to open source projects everyday.



fedora KONFLUX ramalama

We're leading CRA efforts in Open Source Communities and EU Official Standardization bodies to make sure the open-source ecosystem is CRA-compliant and healthy.

THE LINUX FOUNDATION ECLIPSE FOUNDATION CEN CENELEC ETSI EUROPEAN STANDARDIZATION ORGANIZATIONS

Why OpenSSL should care?

OpenSSL Corporation as a Manufacturer?

- Provider of enterprise open-source cryptographic libraries for the global market, including the EU.
- **Support customers on their path to CRA compliance.**

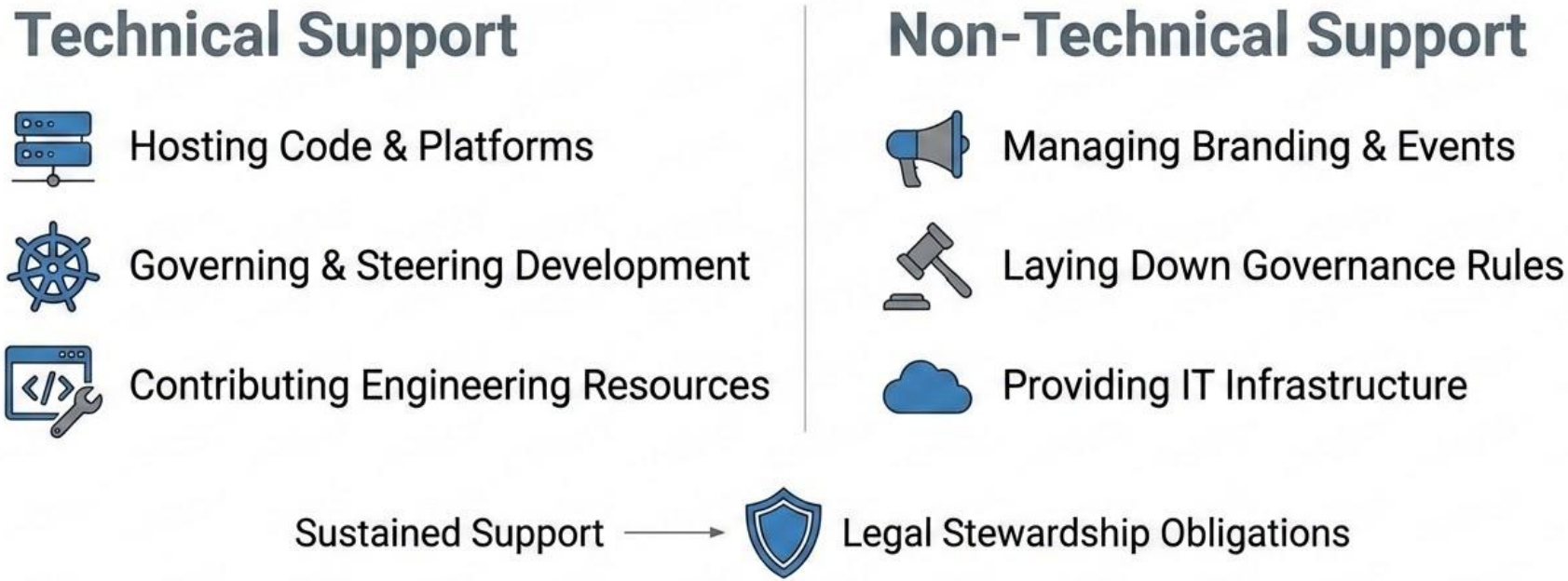
OpenSSL Foundation as a potential Open Source Software Steward

- For OpenSSL projects - OpenSSL, Bouncy Castle...
- For non-OpenSSL projects?
- Does Corporation need to become Steward too???



Committed to Providing Sustained Support

- Stewardship is NOT really a choice



- https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
- https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16959-Draft-Commission-guidance-on-the-Cyber-Resilience-Act_en

Steward is Legally Required To



Red Hat as a Steward for Fedora ensures the sustainability of FOSS and helps following the best secure practices. Full CRA compliance for downstream commercial products, such as Red Hat Enterprise Linux is covered by Red Hat as the Manufacturer.

Red Hat 6 Stewardship Principles

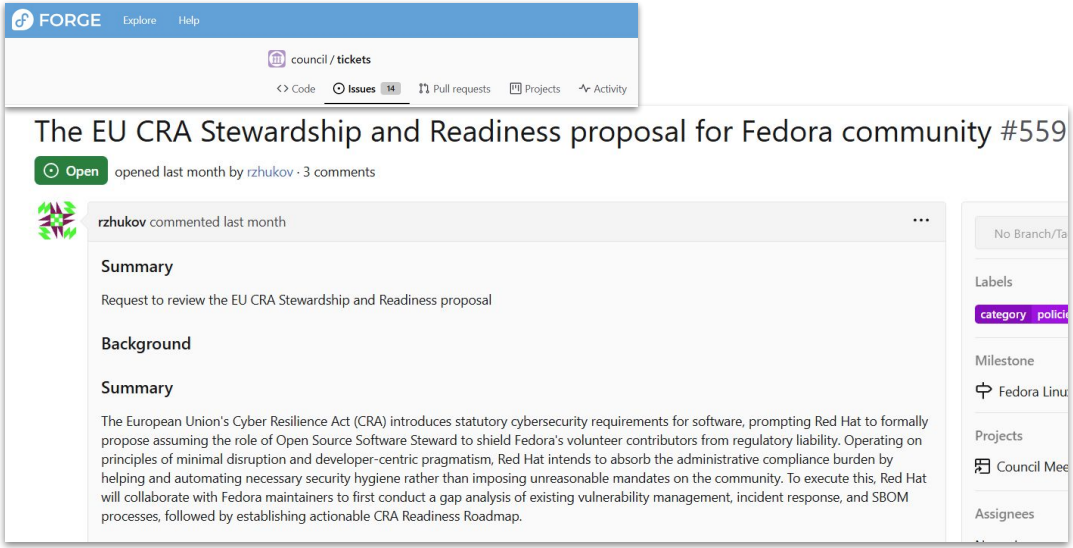
- **Listen First, Act Second**
- **Security First**
- **Pragmatic & Dev-Centric**
- **Minimal Disruption**
- **Gap-Filling Support**
- **Diversity & Tailored Fit**

red.ht/cra-steward

The "Champion Steward"

Going beyond minimum legal obligations for some of the most important projects **world runs on** like **Fedora** to promote top-tier quality and security practices.

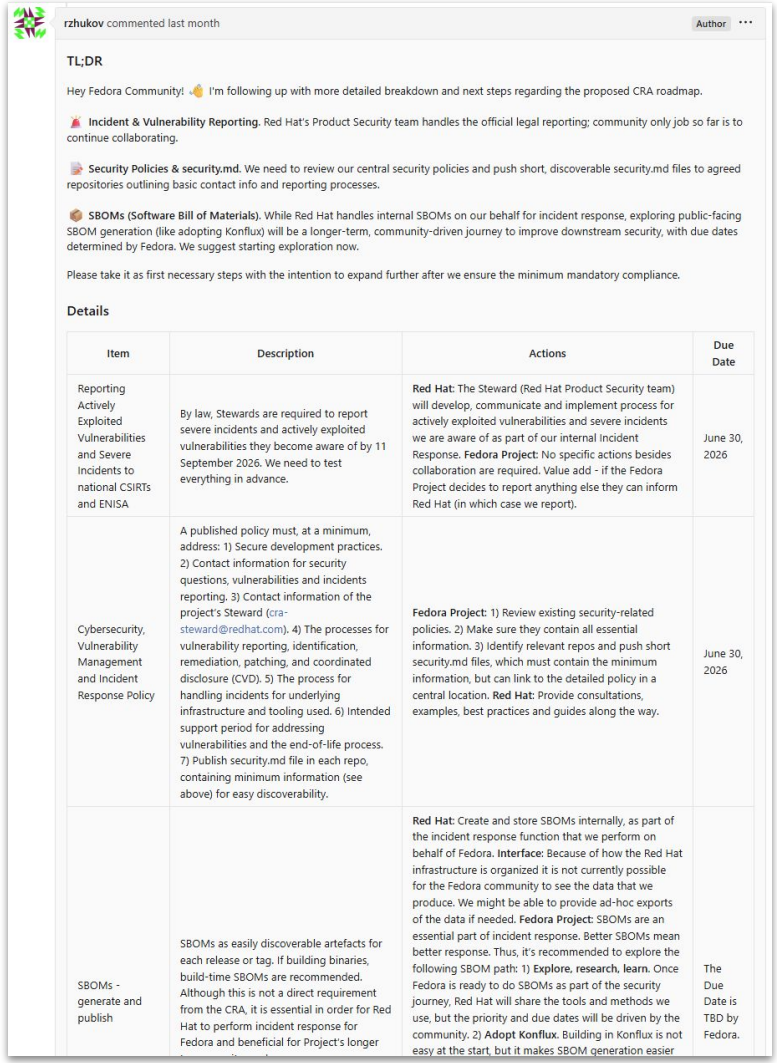
Partnership is the Only Way to Go



forge.fedoraproject.org/council/tickets/issues/559

forge.stg.fedoraproject.org/Rainbows-and-Unicorns/issue_creation_test/issues/99



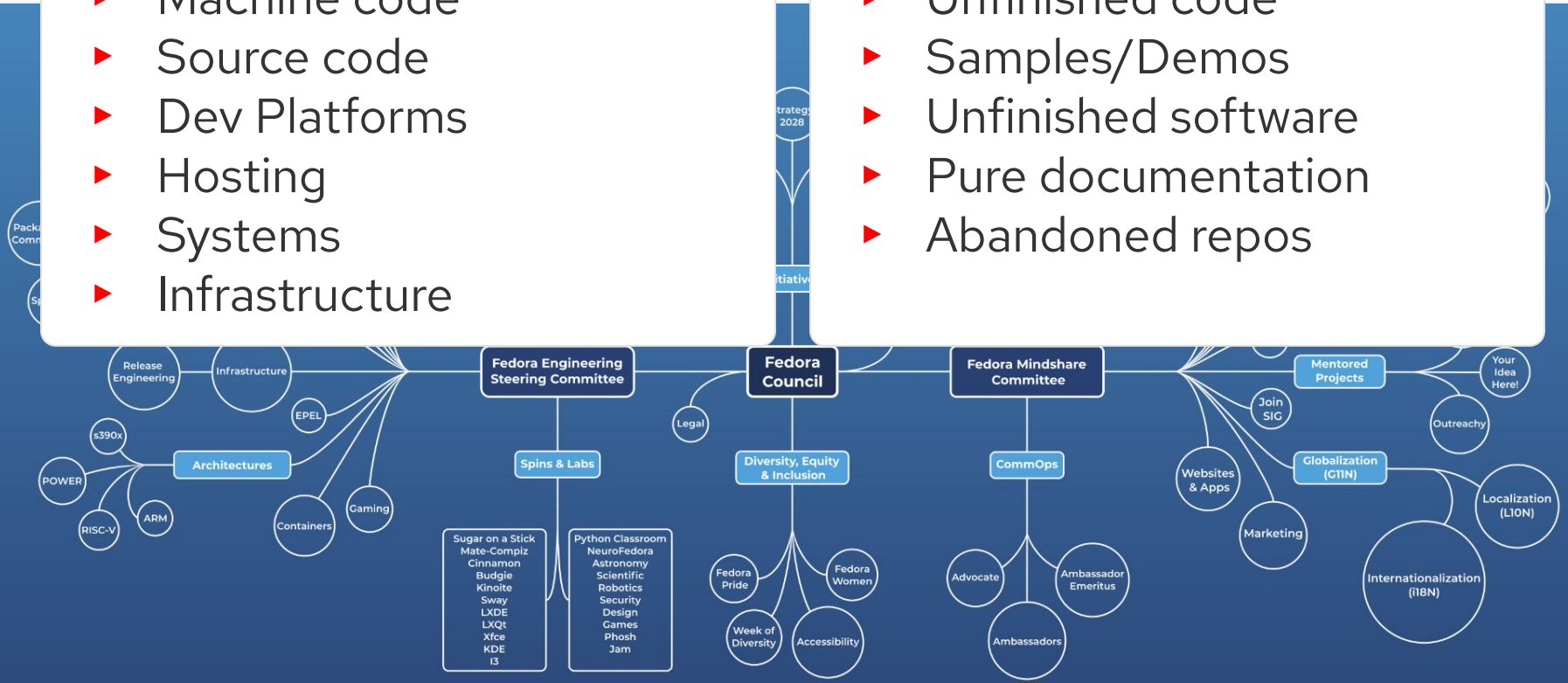


In Scope

- Machine code
- Source code
- Dev Platforms
- Hosting
- Systems
- Infrastructure

Out Of Scope

- Unfinished code
- Samples/Demos
- Unfinished software
- Pure documentation
- Abandoned repos



fedora

Fedora Project Organizational Chart

Last Updated June 2023

~~Requirements~~ Guidelines for Projects

red.ht/cra-steward



Light - to help satisfy Stewardship obligations

- Security Policy (and SECURITY.md)
- Vulnerability Management Process (CVD)
  - Reporting Actively Exploited Vulns
- Incident Response Process (IRP)
  - Reporting Severe Incidents



Red Hat will take care of reporting to to ENISA and local CSIRTs. Reporting starts 11 Sep 2026.



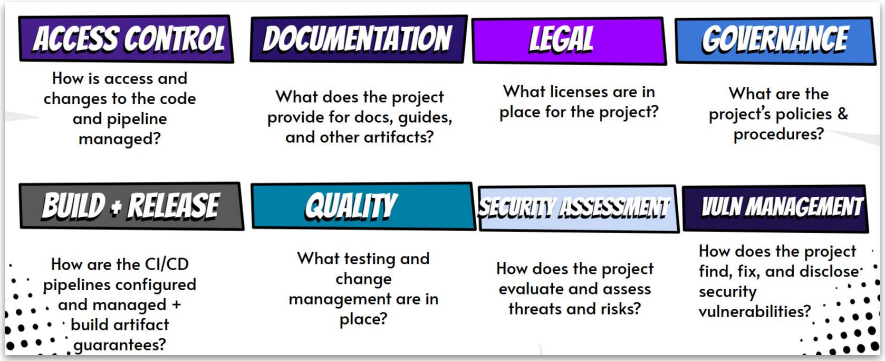
Champion - best practices

- SBOMs
- Security Self-Assessment
- Contributing Guidance
- Release Documentation
- Defect Reporting Guide
- MFA
- Branch Protection
- Licence File
- SLSA - L1
- Signing Commits
- OpenSSF Baseline (OSPS) - L1
- OpenSSF Best Practices - Passing

FOSS maintainer? No obligations!

*"But what I **want** my project to be useful, widely adopted (by users & **manufacturers**) and at best quality and security. I **voluntarily** implement and document good security practices.*

OpenSSF Baseline - 64 requirements x 3 levels of maturity.



github.com/ossf/security-baseline

Learn:

policy.openssf.org/CRA/maintainers.html

This project voluntarily documents its security practices.

This information is provided "as is", without warranties or guarantees.

The maintainers and contributors:

- have no obligations under the EU CRA;
- are not Manufacturers, Importers, or Economic Operators;
- assume no financial, contractual, or legal liability;
- and do not provide CRA compliance assurances.

Entities incorporating this software into commercial products remain solely responsible for regulatory compliance, risk assessment, and vulnerability management.

If you have any additional questions contact: cra-steward@redhat.com

How to React as a Maintainer

What you might hear from your project consumers:

"Are you CRA compliant?"

"As part of our CRA audit - here are the issues we found in your OSS project we give you 1 month to fix"

"I offer you to become OS SW Steward for your project"

Collaborate

Consider it as an opportunity. Express clearly how others can help your project.

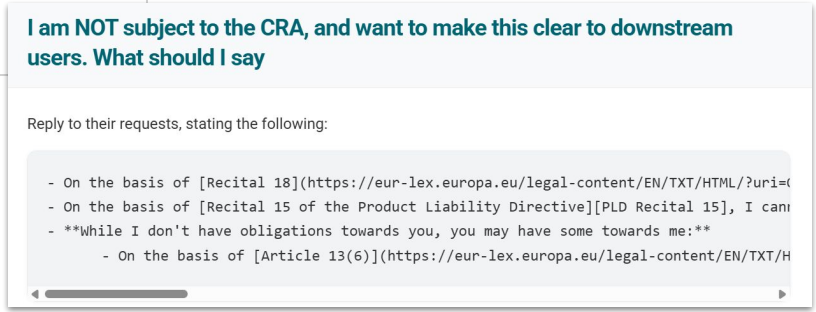
Gentle Response

Provide a gentle "I'm not your supplier" response. Don't sign compliance declarations.

Maintain Autonomy

You have no obligation to accept a stranger as a Steward.

cra.orcwg.org/faq/



I am NOT subject to the CRA, and want to make this clear to downstream users. What should I say

Reply to their requests, stating the following:

```
- On the basis of [Recital 18](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=(
- On the basis of [Recital 15 of the Product Liability Directive][PLD Recital 15], I can
- **While I don't have obligations towards you, you may have some towards me:**
      - On the basis of [Article 13(6)](https://eur-lex.europa.eu/legal-content/EN/TXT/H
```

All That We Do is Upstream

ECLIPSE FOUNDATION

Open Regulatory Compliance



orcwg.org/cra/resources/d3-5-white-paper-on-open-source-software-stewards-and-cra/

THE LINUX FOUNDATION

OpenSSF



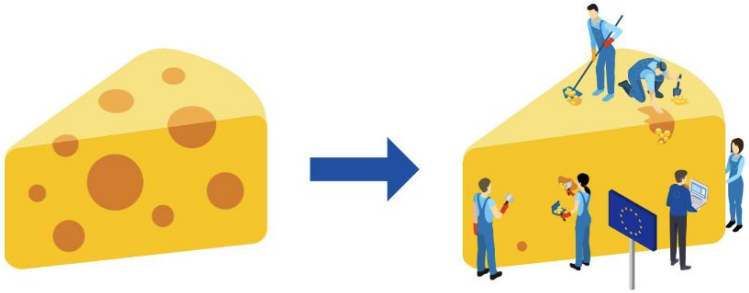
policy.openssf.org/CRA/stewards-playbook.html

Red Hat





red.ht/cra-steward



European Commission

OSS Project 1

Fixes

Steward

Help

Manufacturer

Consumer or Partner

PDE

Fixing Update

Vulnerability

OSS Project N

The FOSS Guidance

10 pages of FAQ on FOSS and CRA, for eg

- 3.1 Determining if free and open-source software is under one's responsibility
- 3.2.1 Charging a price
- 3.2.3 Support services
- 3.4 Contributors and downstream uses



Commission publishes new guidance to support timely Cyber Resilience Act implementation

POLICY AND LEGISLATION

Publication 27 July 2026

Learn:

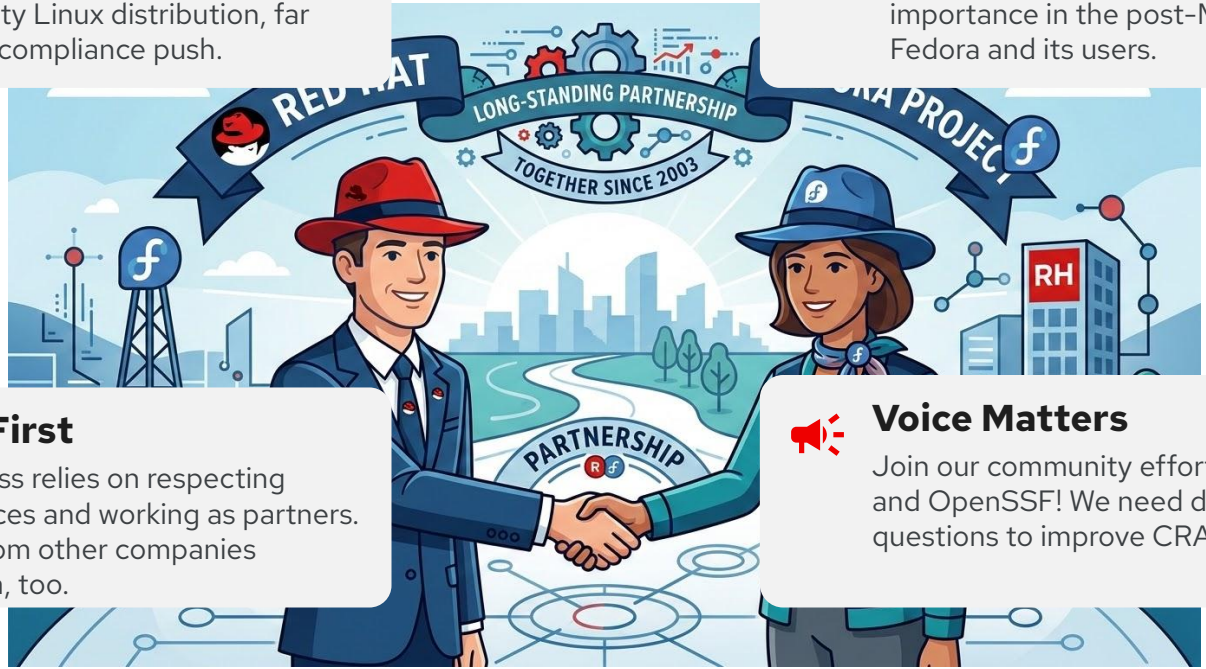
https://digital-strategy.ec.europa.eu/en/library/commission-publishes-new-guidance-support-timely-cyber-resilience-act-implementation

Quality & Compliance

CRA is a bridge to a superior security posture for the best quality Linux distribution, far beyond a simple compliance push.

Heightened Awareness

Security is at its peak visibility and importance in the post-Mythos era. Vital for Fedora and its users.



Community First

Sustainable success relies on respecting community practices and working as partners. We expect that from other companies supporting Fedora, too.

Voice Matters

Join our community efforts at Eclipse ORC and OpenSSF! We need diverse voices and questions to improve CRA. For all.

The Opportunity is Now

Tell us: which security problems are most challenging for you? Let’s work on them together.

Featured Links

Resource	Link
CRA Full Text	eur-lex.europa.eu/eli/reg/2024/2847/oj
CRA Implementation Portal, incl. FAQ (Commission)	digital-strategy.ec.europa.eu/en/factpages/cyber-resilience-act-implementation
Draft CRA Guidance	digital-strategy.ec.europa.eu/en/news/commission-publishes-feedback-draft-guidance-assist-companies-applying-cyber-resilience-act
ENISA Single Reporting Platform (SRP)	https://www.enisa.europa.eu/topics/product-security-and-certification/single-reporting-platform-srp
Red Hat CRA Page (links to blogs and materials)	red.ht/cra-ext
CRA Standards Educational Portal	www.stan4cra.eu
ETSI Standards Open for Consultation	docbox.etsi.org/CYBER/EUSR/Open
Free CRA Basics Class by Linux Foundation	training.linuxfoundation.org/express-learning/understanding-the-eu-cyber-resilience-act-cra-lfel1001/
OpenSSF Global Cyber Policy WG	github.com/ossf/wg-globalcyberpolicy
Eclipse Open Regulatory Compliance WG	github.com/orcwg
OpenSSF CRA Voluntary Guide for FOSS Maintainers	policy.openssf.org/CRA/maintainers.html
OpenSSF Stewards Playbook	policy.openssf.org/CRA/stewards-playbook.html
OpenSSF Maintainers Guide	policy.openssf.org/CRA/maintainers.html
OSPS Baseline	baseline.openssf.org
Kunflux - Trusted SoftwareFactory	github.com/konflux-ci