The CRA and what it means for us

Greg Kroah-Hartman

gregkh@linuxfoundation.org
git.sr.ht/~gregkh/presentation-cra

Disclaimer

All of this is just my personal opinion, based on working as part of CRA expert group.

"Us" means "Open Source developers", not "manufacturers" or "businesses" or any other corporate role. I'm only going to focus on how this all will affect us individual developers in our role of creating software that everyone else uses.

The CRA has loads of TLAs

- Cyber Resiliance Act (CRA)
- Product with digital elements (PDE)
- Open Source Software (OSS)
- Software bill of materials (SBOM)
- European Union (EU)

What is the CRA

- EU Regulation covering PDEs in the EU market
- Obligations for manufacturers, distributors, and importers
- Product classification
- Market survelliance and enforcement

Market surveliance and enforcement

- Designated Cyber Security Incident Response Teams (CSIRT)
- European Union Agency for Cybersecurity (ENISA)

What is the CRA – cont.

- Requirements for cybersecurity portions of the PDE lifecycle
- Vulnerability reporting and handling

Software lifecycle requirements

- Risk management
- Design
- Development
- Documentation (SBOM)
- Production

Different “types” of products

- Default
- Level 1
- Level 2
- Critical

Stuff outside the scope of the CRA

- Services (websites, SaS)
- Many specific types of devices
  - Auto, medical, aeronautical, marine, etc.
- Non-commercial hobby products

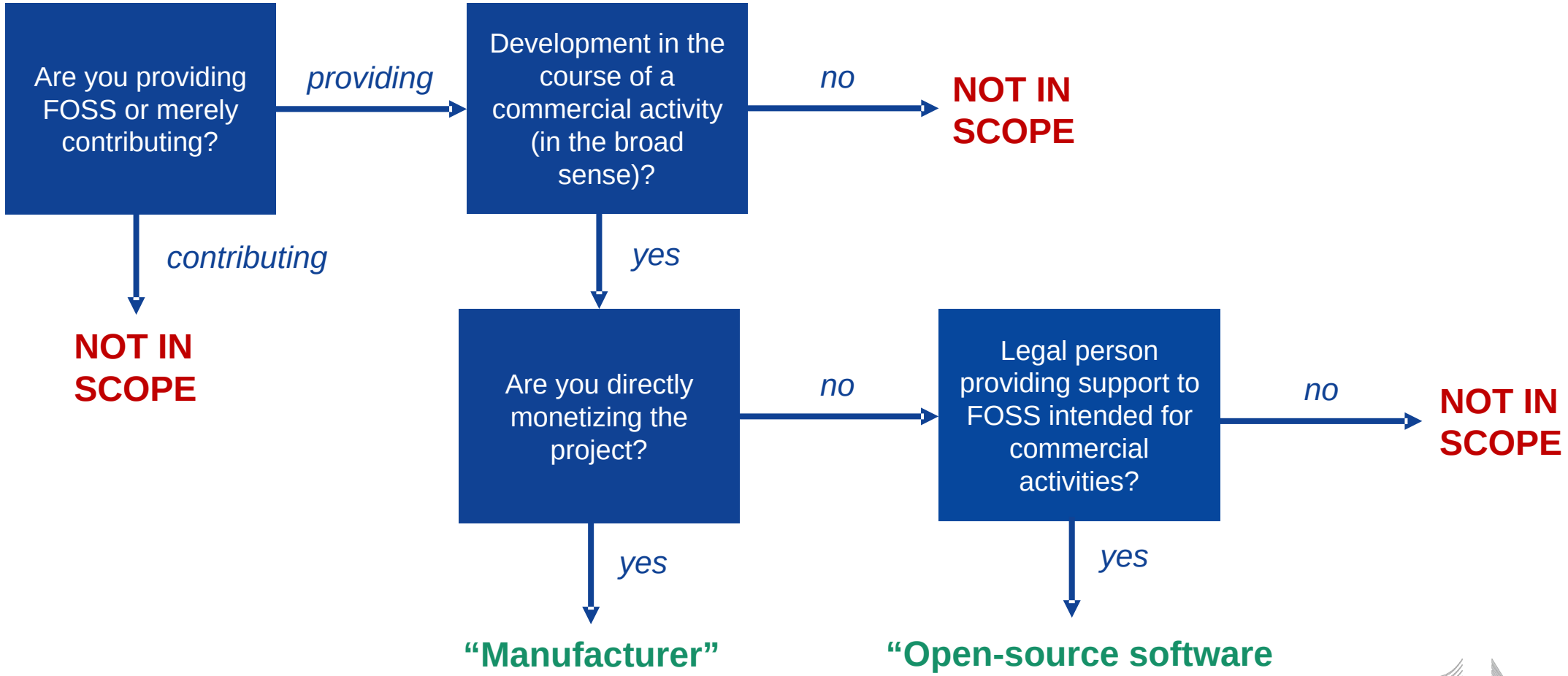
Stuff outside the scope of the CRA

- Services (websites, SaS)
- Many specific types of devices
  - Auto, medical, aeronautical, marine, etc.
- Non-commercial hobby products
  - Until your software gets added to a product!

Different classification of groups

- OSS developers
- OSS “Stewards”
- Manufacturers
- Integrators
- Distributors

Is your open source project covered? *



** Simplified flow-chart for presentation purposes.*

European Commission

Stewards responsibilities

- Provide a contact for security issues
- Report security fixes to <SOMETHING>

You should already be doing this!

- security.txt
- Become a CNA or fill out a web form
- https://bestpractices.dev/
- reuse tool from FSFE

Stewards checklist

https://github.com/ossf/wg-globalcyberpolicy/blob/main/documents/CRA/checklists/OSS_Stewards_Obligations_Checklist.md

Timeline

- 10 December, 2024
  - “entered into force”
- 11 June 2026
  - Governments ready
  - Assesment bodies ready

Timeline – cont.

- 11 September 2026
  - Manufacturers must report
- 11 December 2027
  - Entire regulation applies

Standards

- Use of standards is voluntary
- Standards are not finished yet
- Some will not be finished until after Dec, 2027

Resources

- Linux Foundation CRA site
- Linux Foundation free CRA training course
- OpenSSF documentation
- ENISA documentation

The CRA and what it means for us

Greg Kroah-Hartman

gregkh@linuxfoundation.org
git.sr.ht/~gregkh/presentation-cra