THE CRA IS AN OPEN SOURCE SUSTAINABILITY LAW

How the CRA can boost Open Source Sustainability

Jordan Maris, OSI

whoami

- Former Lawmaker, worked on the CRA
- OSI EU policy analyst
- Participant in Standardisation process at ETSI/CENCENELEC
- Participant in Commission funded dissemination work on CRA

Before we go any further...

alert!

- To comply with the CRA, most manufacturers will need to follow standards.
- OSI has fought to make sure the Open Source community gets a say in these standards.
- You can review and comment on domain specific standards!
- We need your help!

Available Standards

- Password Managers
- Antivirus
- VPNs
- Network Management Systems
- Boot Managers
- PKI
- Network Interfaces
- Operating Systems
- Routers, Modems & Switches
- Virtualisation, Containers, Hypervisors
- Smart Appliances

Co-funded by EFTA

Co-funded by the European Union

Participate through Public Participation Platform

- ETSI has set up a public platform for the purpose of collecting feedback from the Open Source Community.
- The platform, built on gitlab, allows you to Open Issues on the standards.
- Find it here: https://labs.etsi.org/rep/stan4cra

Co-funded by EFTA

Co-funded by the European Union

Join upcoming deep-dive sessions

- Deep-dive sessions will be organised for each standard.
- We will communicate the dates ASAP on the page linked in the QR code!
- 2 hours with the rapporteurs

Co-funded by EFTA

Co-funded by
the European Union

THE CRA IS AN OPEN SOURCE SUSTAINABILITY LAW

How the CRA can boost Open Source Sustainability

Jordan Maris, OSI

tl;dr:

- we added new things to the CRA
- it is not yet clear what these things will become
- but they are a massive opportunity for the open source ecosystem to solve our sustainability problems

A quick recap of the CRA:

- September 2022: CRA proposed, it's bad for Open Source
- September 2022 - December 2023: OSI and others fight to fix it.
- March 2024: EU agree on final text, which:
  - Exempts non-commercial FOSS
  - creates *Open Source Software Stewards*
  - creates *attestation programmes*

The three actors in the CRA ecosystem

Manufacturers

companies who make products with digital elements and sell them on the EU market.

Open Source Software Stewards

Newly created, their exact purpose and form is still to be determined

Devs of non-commercial Open Source

Exempted entirely from the law, they have no obligations, however users of their code might...

what is a software steward?

good question

Open Source Software Stewards

Support development

of an FOSS project intended for use in Commercial products, through hosting, developer hours or financial support (examples).

Handle Vulnerability reports

An Open Source Software steward **must** handle vulnerability reports for that FOSS project, or have a means to handle these reports.

Decide Cybersecurity rules

An Open Source Software Steward **must** set out a Cybersecurity policy for the project.

Commonly Asked Steward Questions

- **Will the law force me to be a steward?**
- **Do all Open Source projects need a steward?**
- **Can a manufacturer be an Open Source steward, too ?**
- **What happens when a steward misbehaves?**

The Eclipse Foundation has launched the Open Regulatory Compliance Working group, a group focused on helping Open Source projects comply with laws including the CRA. They have a full Q&A for the CRA here! Check out https://**cra.orcwg.org**/

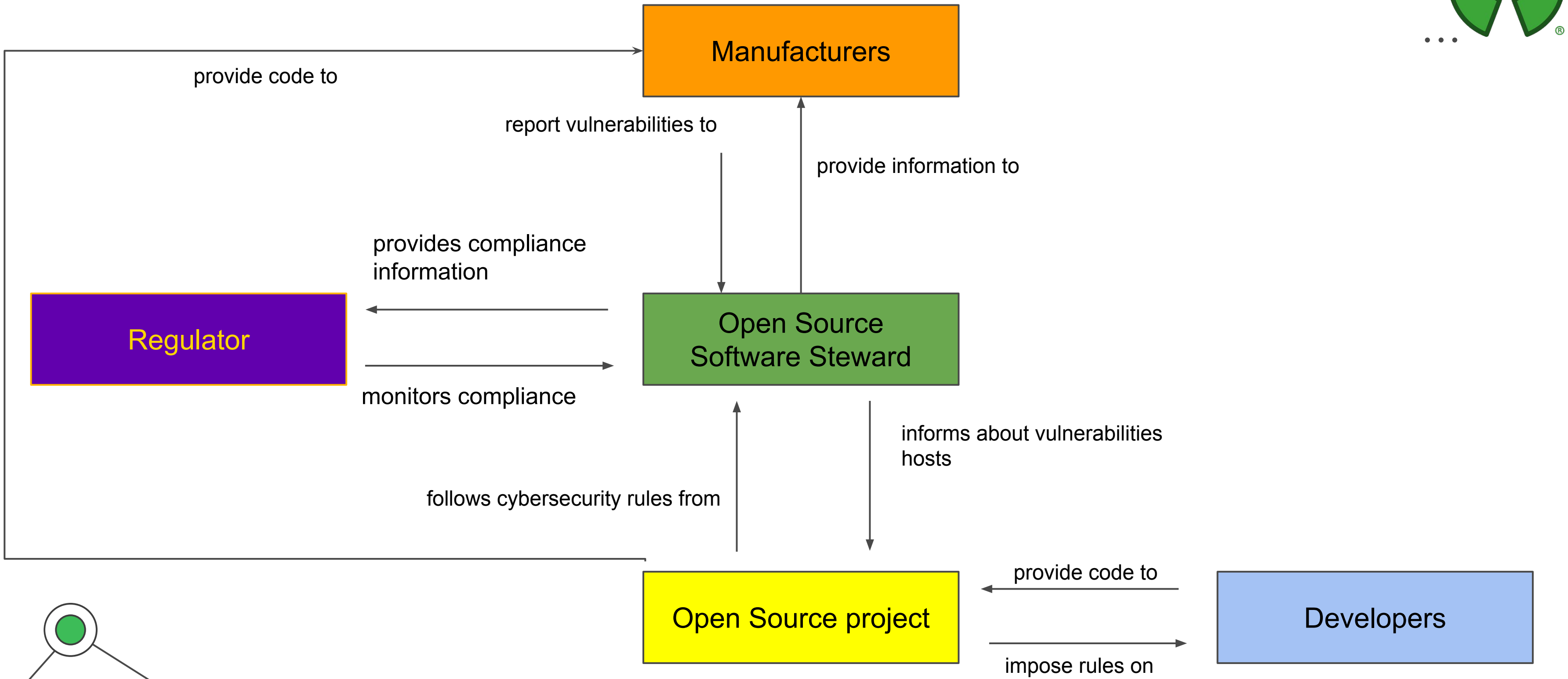
Why be a software steward?

- Lightweight requirements compared to manufacturers (in theory)
- Exempted from fines under the CRA
- Could help strengthen adoption of the FOSS project

What will stewards look like in practice?

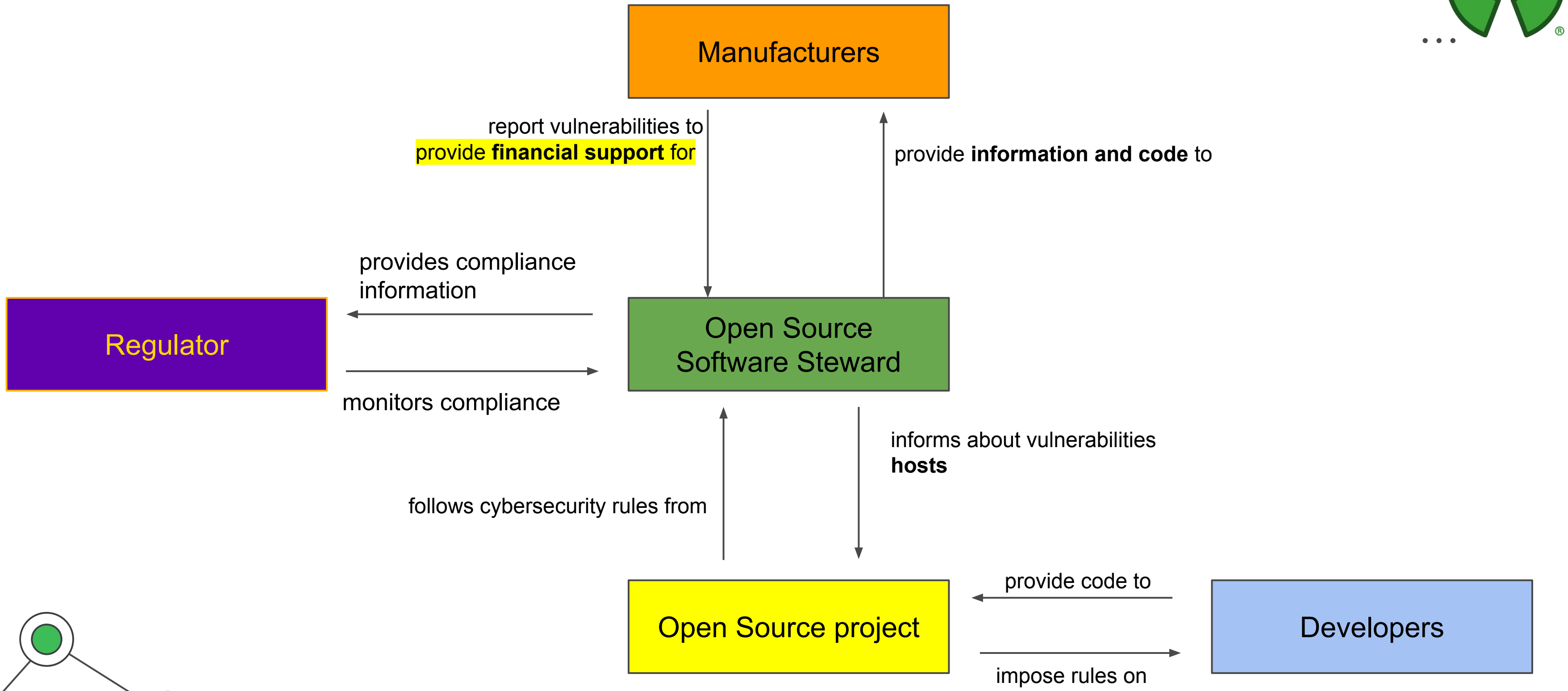
- Open Source Foundations.
- Companies working together due to a common interest in a FOSS project.
- Open Source Companies with community editions.
- Individuals who want to create an entity to host their FOSS project.

What could Stewards Look like? v1


Manufacturers
provide code to
report vulnerabilities to
provide information to
provides compliance information
Regulator
Open Source Software Steward
monitors compliance
informs about vulnerabilities hosts
follows cybersecurity rules from
provide code to
Open Source project
Developers
impose rules on

This doesn’t benefit us much..

What could Stewards Look like? v2



Manufacturers

report vulnerabilities to
provide **financial support** for

provide **information and code** to

Regulator

provides compliance information

monitors compliance

Open Source Software Steward

follows cybersecurity rules from

informs about vulnerabilities
hosts

Open Source project

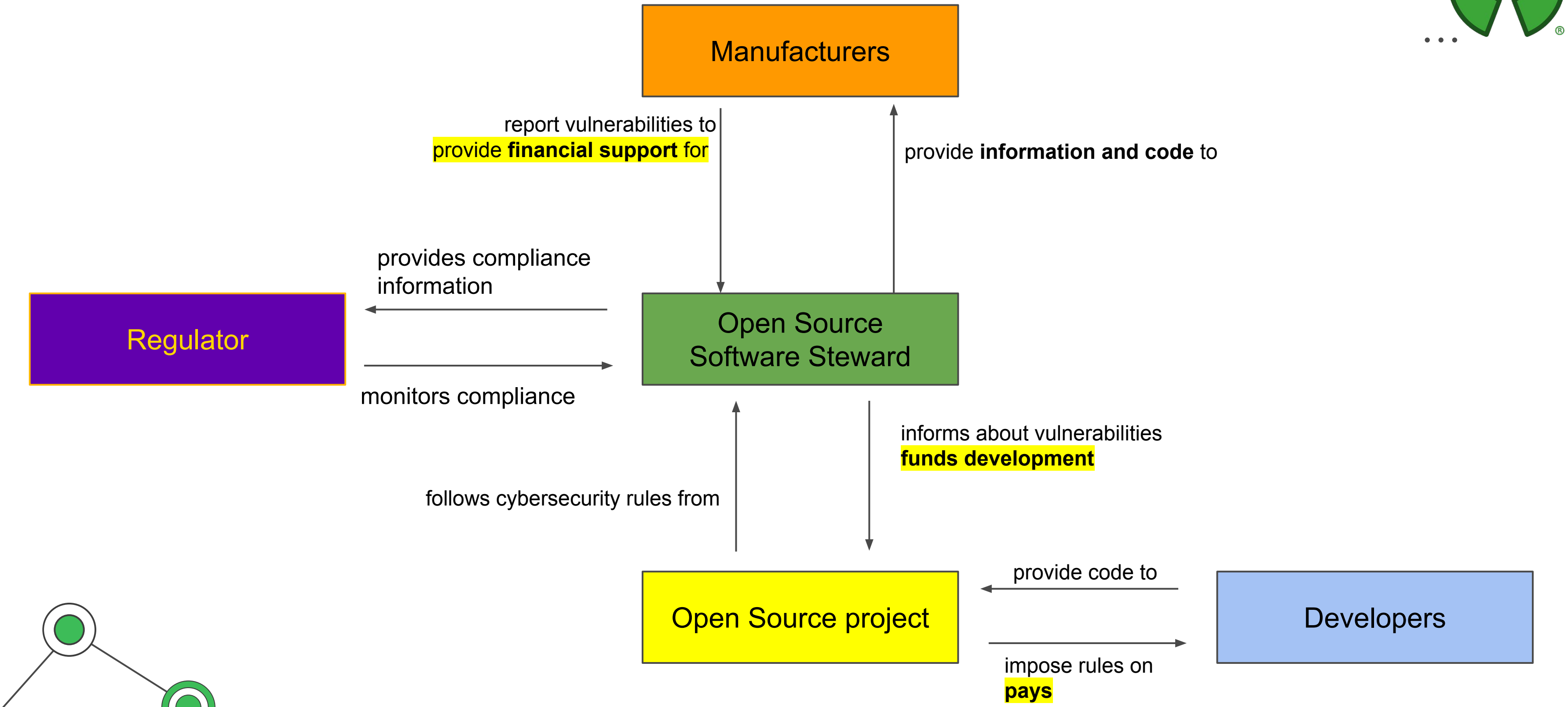
provide code to

impose rules on

Developers

It could be better...

What could Stewards Look like? v3



Manufacturers

report vulnerabilities to
provide **financial support** for

provide **information and code** to

provides compliance
information

Regulator

Open Source
Software Steward

monitors compliance

informs about vulnerabilities
funds development

follows cybersecurity rules from

provide code to

Open Source project

Developers

impose rules on
pays

but why would manufacturers fund software stewards?

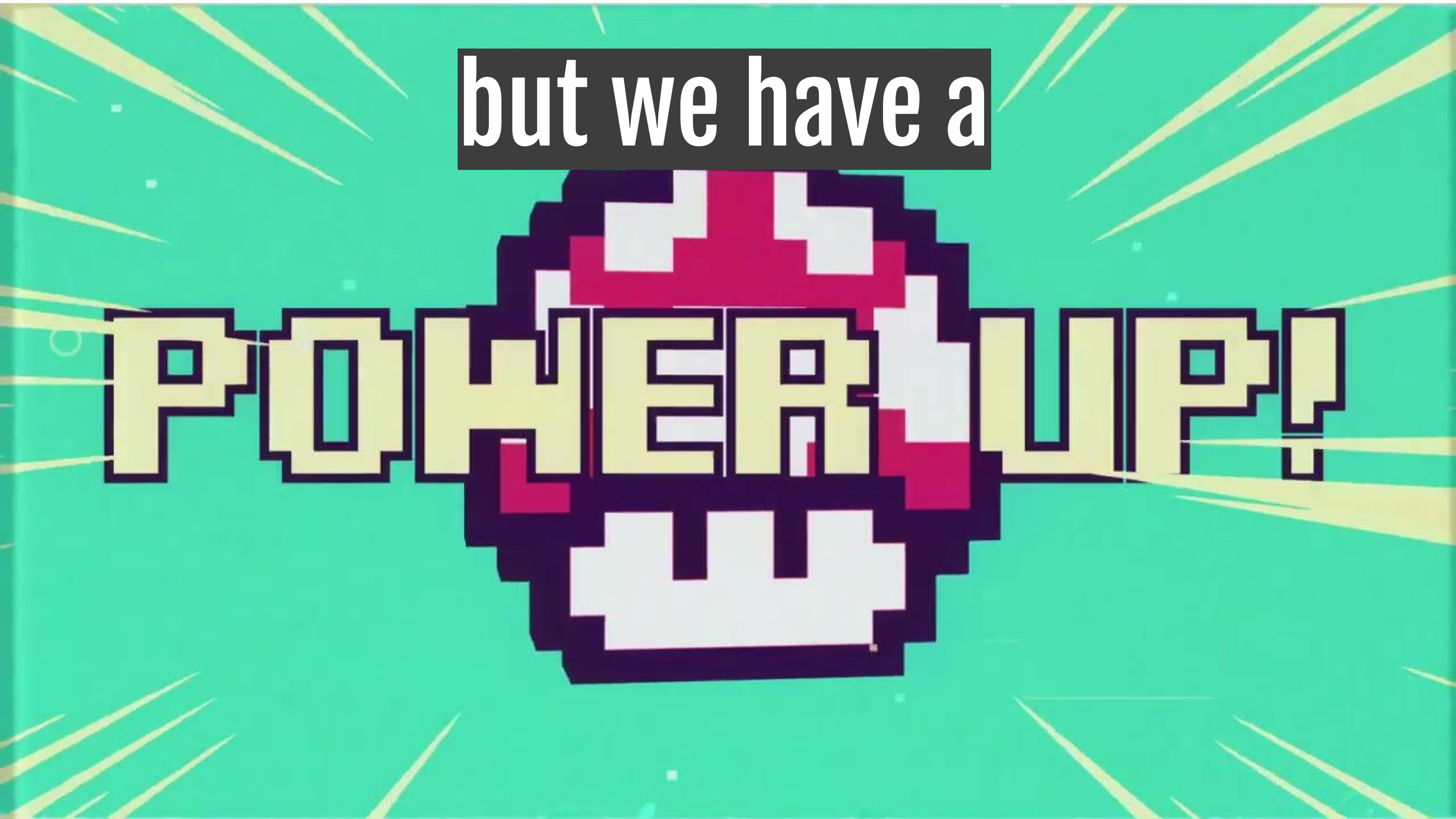
Manufacturer Requirements

- Due diligence on use of third-party components:
    - No guidelines yet, but this probably implies at least one of the following:
        - Checking project governance
        - Getting information about the project for compliance purposes.
        - Checking code and software capabilities

is this enough alone?

probably not

but we have a



introducing *security attestations*

ART 25 CRA

In order to facilitate the due diligence obligation set out in Article 13(5), in particular as regards manufacturers that integrate free and open-source software components [the Commission is empowered to **establish voluntary security attestation programmes allowing the developers or users of products with digital elements qualifying as free and open-source software as well as other third parties to assess the conformity of such products with all or certain essential cybersecurity requirements laid down in this Regulation.**]

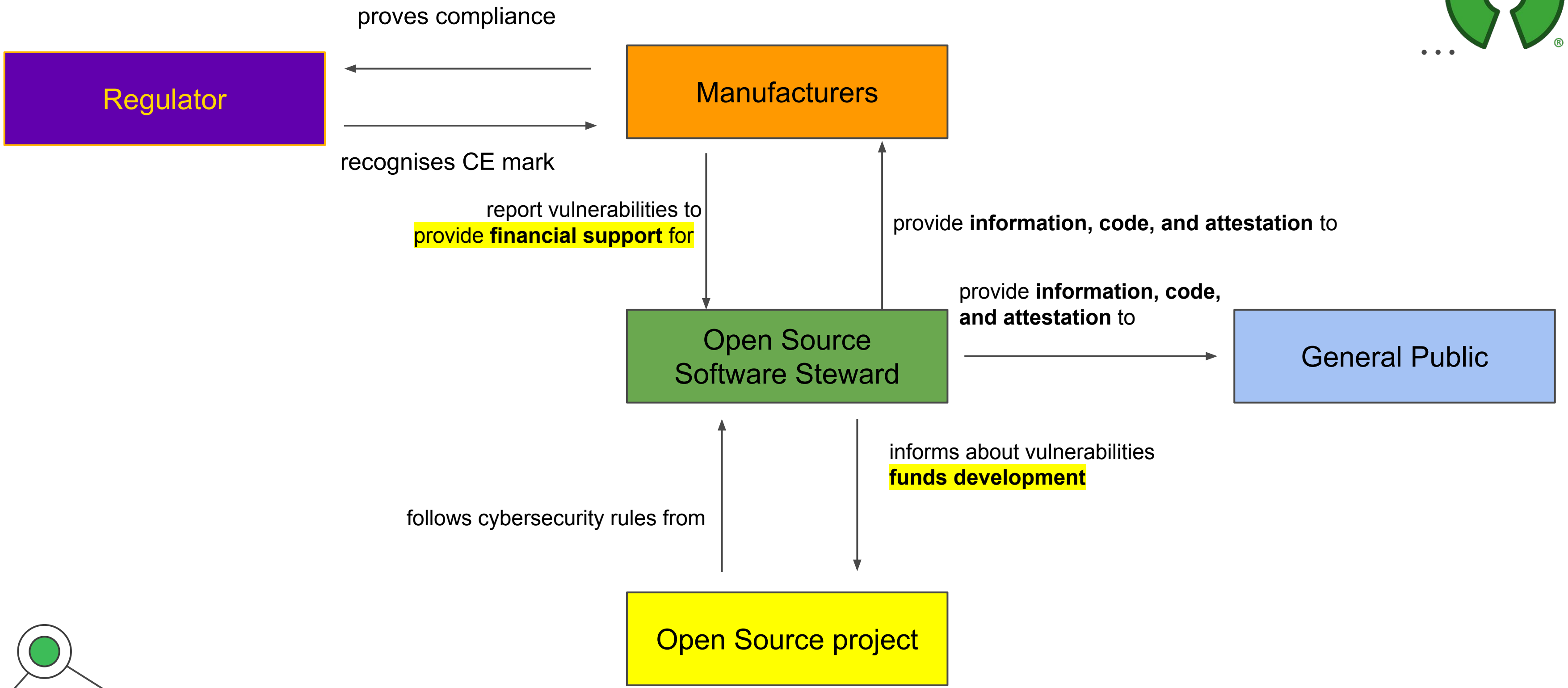
Benefit of Attestations

- **Immediately fulfils due-diligence requirements for manufacturers.**
- **Improves security and security practices of Open Source projects.**
- **Potential source of revenue for Open Source Projects.**

Potential Pitfalls

- Third parties doing attestations for projects they do not participate in, selling them and syphoning off the money.
- Cost of attestations negating the benefits of Open Source.
- Freeriding.

Possible Models: 1



proves compliance

Regulator

Manufacturers

recognises CE mark

report vulnerabilities to
provide **financial support** for

provide **information, code, and attestation** to

provide **information, code,**
and attestation to

Open Source
Software Steward

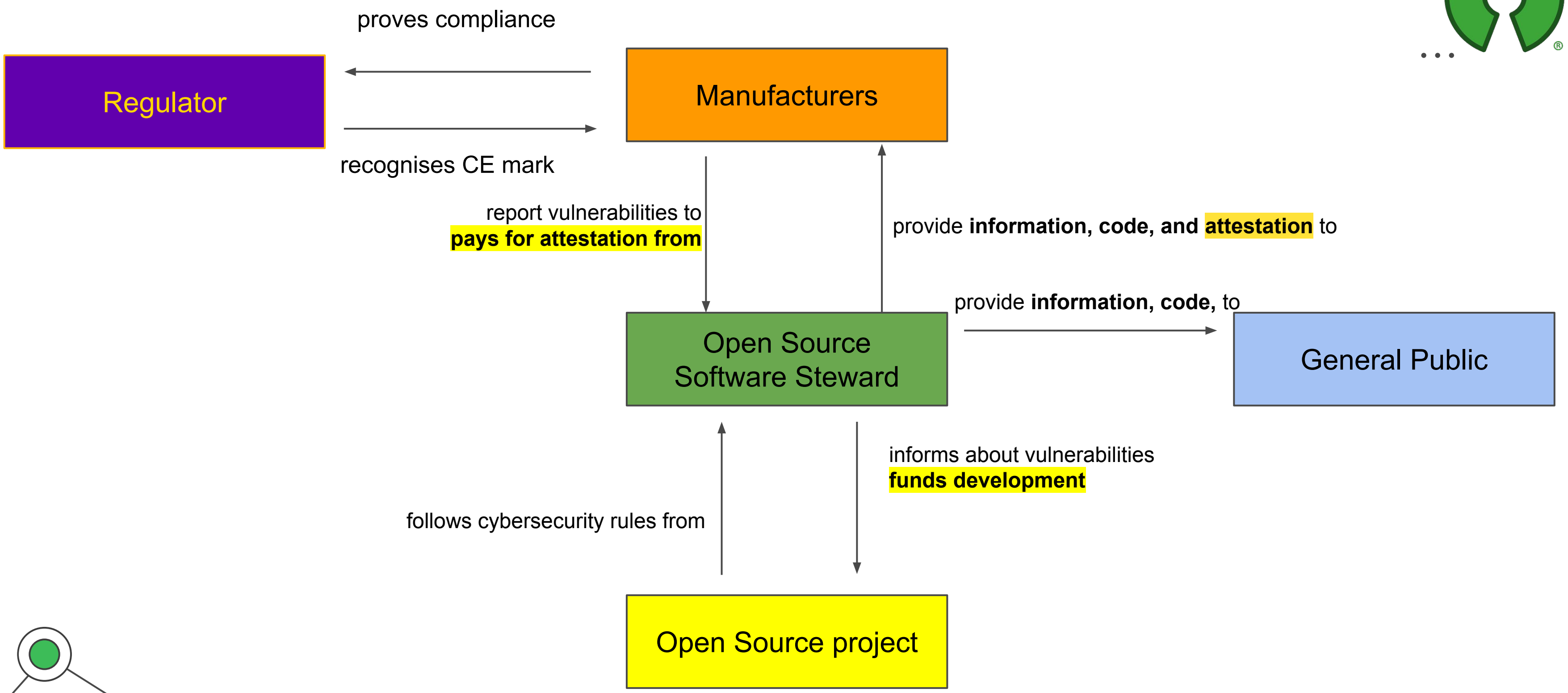
General Public

informs about vulnerabilities
funds development

follows cybersecurity rules from

Open Source project

Possible Models: 2



proves compliance

Regulator

Manufacturers

recognises CE mark

report vulnerabilities to
pays for attestation from

provide **information, code, and attestation** to

Open Source
Software Steward

provide **information, code,** to

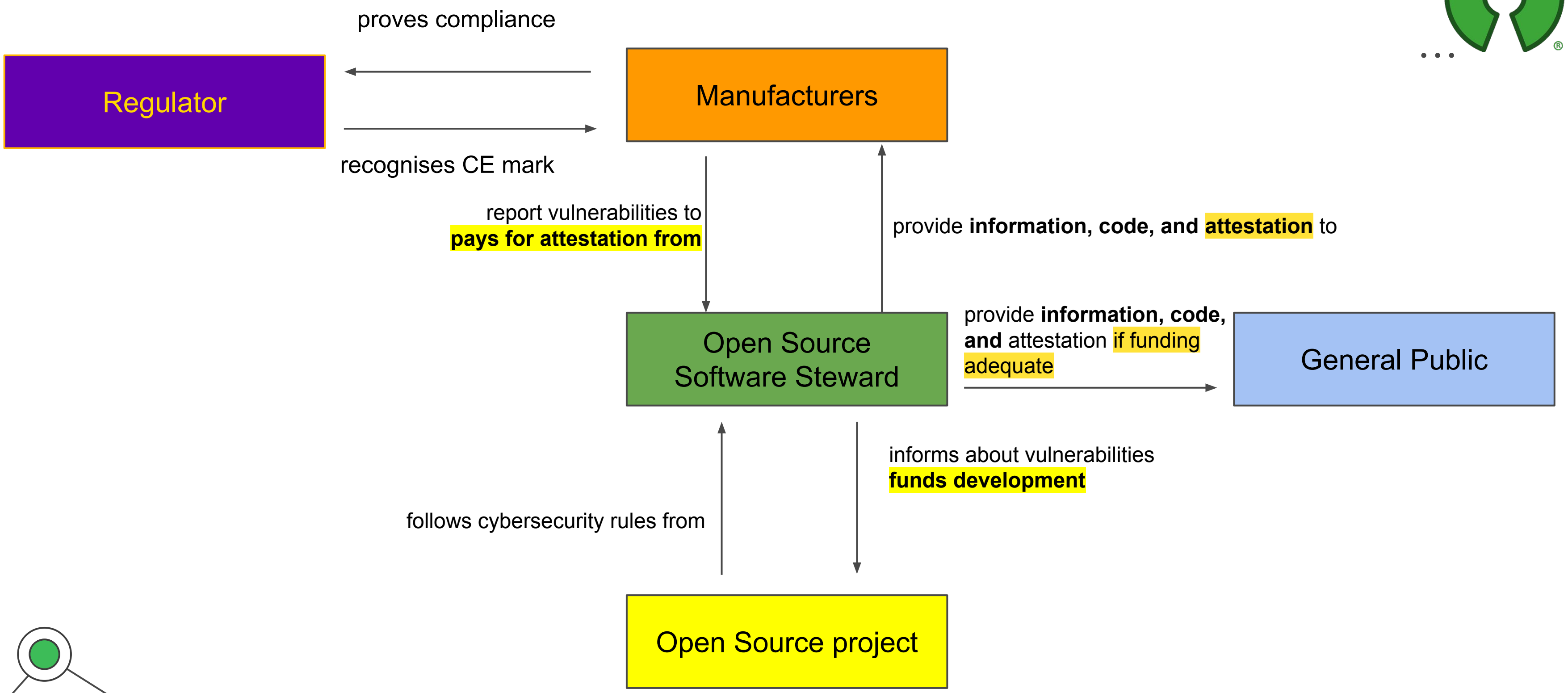
General Public

informs about vulnerabilities
funds development

follows cybersecurity rules from

Open Source project

Possible Models: 2 (Variant)



proves compliance

Regulator

Manufacturers

recognises CE mark

report vulnerabilities to
pays for attestation from

provide **information, code, and attestation** to

Open Source Software Steward

provide **information, code, and** attestation if funding adequate

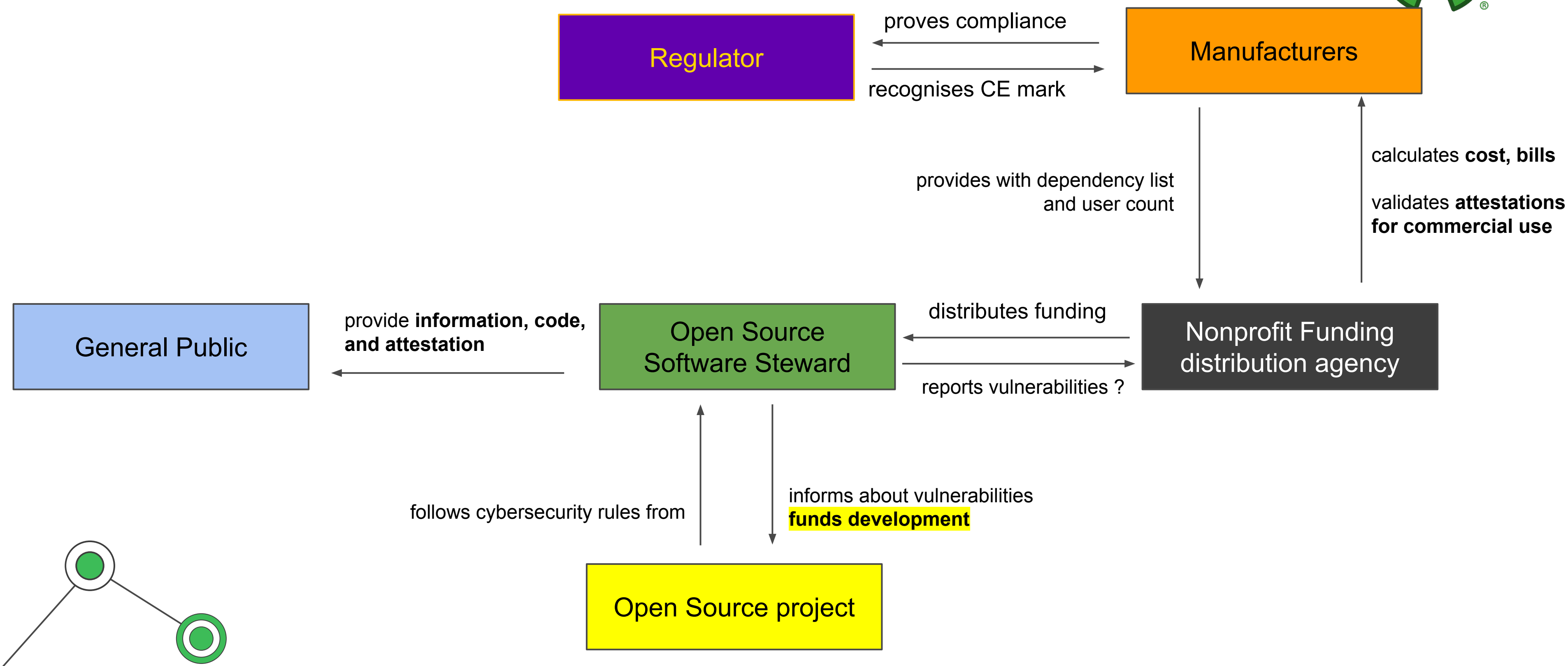
General Public

informs about vulnerabilities
funds development

follows cybersecurity rules from

Open Source project

Possible Models: 3


Regulator
proves compliance
recognises CE mark
Manufacturers
provides with dependency list
and user count
calculates **cost, bills**
validates **attestations for commercial use**
General Public
provide **information, code, and attestation**
Open Source Software Steward
distributes funding
reports vulnerabilities ?
Nonprofit Funding distribution agency
follows cybersecurity rules from
informs about vulnerabilities
funds development
Open Source project

all of these models offer a way
to fund Open Source Software

but we have to find the best
model for our ecosystems

none are perfect, but the CRA will happen with or without us...

we need your help! get involved:

github.com/orcwg/cra-attestations

Immediately following this talk
in Crane Hall – Workshop A:

From Brussels with love: Open Source Policy in the EU

questions?