A Theory of Voluntary Security Attestations

Could compliance cost-savings sustain open source software communities?

ÆVA BLACK
NULLPOINT.STUDIO

Agenda

- background
- overview of regulation
- current progress
- predicted challenges
- how to get involved

Innovation → Regulation

2023 U.S. Nat'l Cyber Security Strategy

OBJECTIVE 3.3:
SHIFT LIABILITY FOR INSECURE SOFTWARE PRODUCTS AND SERVICES

Responsibility must be placed on the stakeholders most capable of taking action to prevent bad outcomes, not on the end-users that often bear the consequences of insecure software nor on the open-source developer of a component that is integrated into a commercial product.

OSS Stewards:
a new legal actor

Article 3: Definitions

(13) '**manufacturer**'

means a 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 its name or trademark**, whether for payment, monetisation or free of charge;

(14) '**open-source software steward**'

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

Remember – no effect on personal expression, hobby projects, etc, nor on specifically-regulated industries

Obligations

Stewards ...

Publish documentation regarding:

- Cybersecurity policy relevant to use in digital products.
- Vuln handling policy, including how downstream can report & subscribe.

Willingness and capacity to:

- Cooperate with European and Nat'l market surveillance authorities.
- Notify ENISA and Nat'l CSIRT of any severe incident affecting project infrastructure.
- Notify affected / known users of severe incidents & vulns with downstream effects.

Manufacturers ...

Article 13(5)

Exercise **diligence** when integrating FOSS.

Article 13(6)

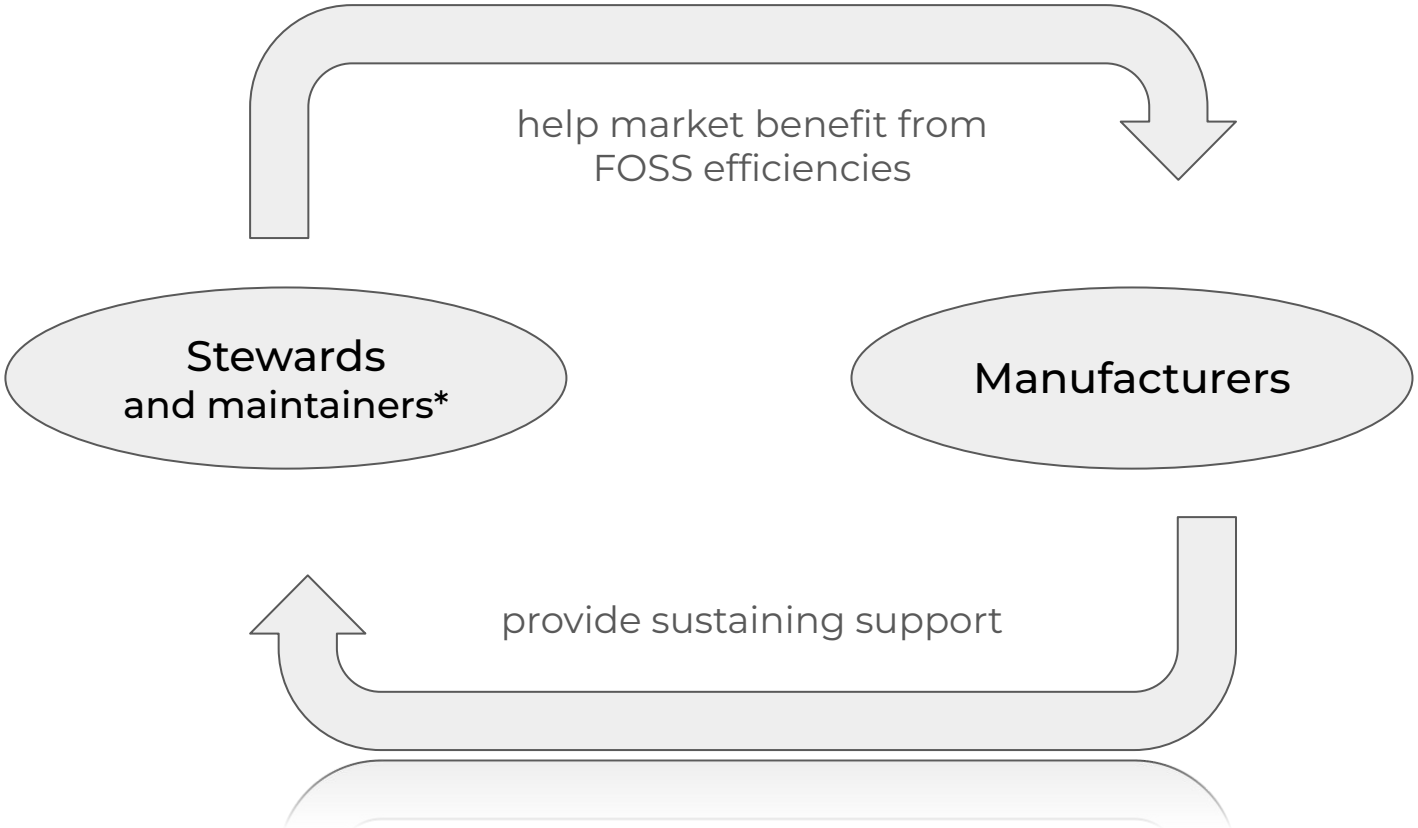
Report vulnerabilities discovered in FOSS & **share remediations** developed for FOSS, even from non-commercial sources.

Article 13(7)

Include FOSS in risk assessment.

Article 13(8)

Handle vulns in FOSS dependencies throughout the product lifecycle..



Article 25
Voluntary Security Attestations

In order to facilitate the due diligence obligation … [of] manufacturers … the Commission is empowered to adopt delegated acts … establishing voluntary security attestation programmes allowing the developers or users of … free and open-source software … to assess the conformity … with all or certain essential cybersecurity requirements … laid down in this Regulation.

We Have Some Questions ...

project URL –
github.com/orcwg/cra-attestations/blob/main/proposals/gen-two-tier-approach.md

relevant questions also here –
cra.orcwg.org/pending-guidance/

Goals

- reduce market burden of re-assessing every FOSS component in every product
- support shared responsibility of maintaining FOSS
- account for projects of all sizes and maturity levels

Progress

October - January

Proposal Developed:

- Tiered Model
- Due Diligence

Questions Clarified:

- Financial Mechanism
- Transitive Dependencies
- Third Party Attestations

Two Tiers – “lite” & “heavy”

lite ...

based on the reasonably foreseeable capabilities of projects that...

- do not have significant commercial support;
- are components and libraries
- are similar to “Default” products

heavy ...

based on the reasonably foreseeable capabilities of projects that...

- benefit from significant commercial support,
- are functionally equivalent to commercial products that would require Module B+C or H assessment
- contain cryptographic algorithms or are intended for use in “Important” or “Critical” products

lite ...

- useful for FOSS that is not product-like, e.g. when use case is *unknowable*
- requires minimal time investment
- easily verifiable
- based on BSI doc TR-03185-2
- similar to SSDF & SLSA

heavy ...

- relies on CRA “Vertical” standards to help Manuf. achieve products’ “presumption of conformity”
- requires expertise and substantial time investment
- recipients may benefit from add’l compliance, e.g. SSDF, ISO27001

Sample Template "Lite"

```
Governance
- [ ] GV.01: The Project must include a contribution guideline.
      Documentation Link:     _____________________________________________
- [ ] GV.02: The Project's contribution guideline should set a
      quality standard for contributions. Check this box to confirm.
- [ ] GV.03: The Project must include documentation about its usage and
      intended purpose or functionality.
      Documentaiton Link:     _____________________________________________

Licensing
- [ ] LE.01: All Project components, including binaries and documentation,
      must be publicly available under an open source license.
      License File Link:      _____________________________________________
- [ ] LE.02: The Project's dependencies, including requirements for
      reproducing the project's distributed binaries, should available under
      an open source license. If this is true, check this box.
      If this is not true, please explain: ____________________________

Quality
- [ ] QA.01: The Project must document, or otherwise include a list of,
      all direct third-party dependencies. This list should include
      cryptographically unique identifiers (checksums) where applicable.
      Link to SBOM or lockfile: _____________________________________________
- [ ] QA.02: The Project's source code, including change history, must be
      publicly available.
      Link to source control: _____________________________________________
- [ ] QA.03: The Project must include documentation describing how to file a
      vulnerability report.
      Link to reporting guide:  _____________________________________________
```

https://raw.githubusercontent.com/orcwg/cra-attestations/refs/heads/main/proposals/template-lite.md

But...

several questions remain unanswerable

(we need your help)

- costs & structures for Stewards varies by country
- country-specific legal req's adds community friction
- tax incentives misaligned or indeterminate
- are attestations a "commercial activity"?

Project Status

Where we are –

- bi-weekly meetings @ 1530
- matrix room & mailing list
- github repo

Ways To Contribute –

- review “heavy-weight” PR
- share your challenges & goals

ORC Attestation Survey

Have Your Say

(deadline Feb 3rd!)

CRA creates
“a differentiated, light-touch regulatory regime for F/OSS Stewards”

And Art. 25 enables adoption of a delegated act specifying the mechanisms for voluntary security attestations.

https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16213-European-Open-Digital-Ecosystems_en

Thanks!

Æva Black

Null Point Studio