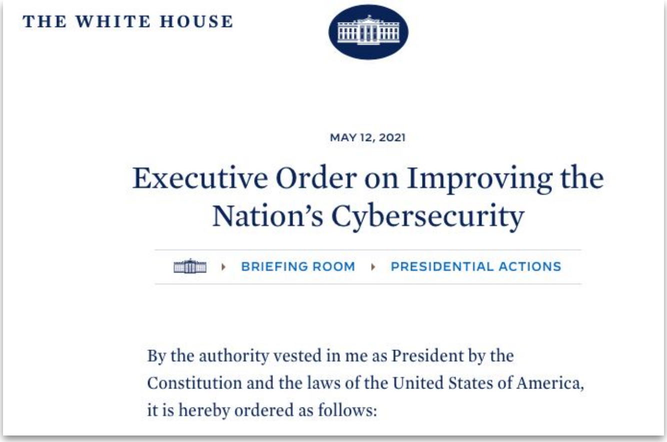
European Cyber Resilience Act: Update for the Eclipse Community

Mike Milinkovich

Executive Director, Eclipse Foundation

July 13, 2023

Legislation is coming our way



THE WHITE HOUSE

MAY 12, 2021

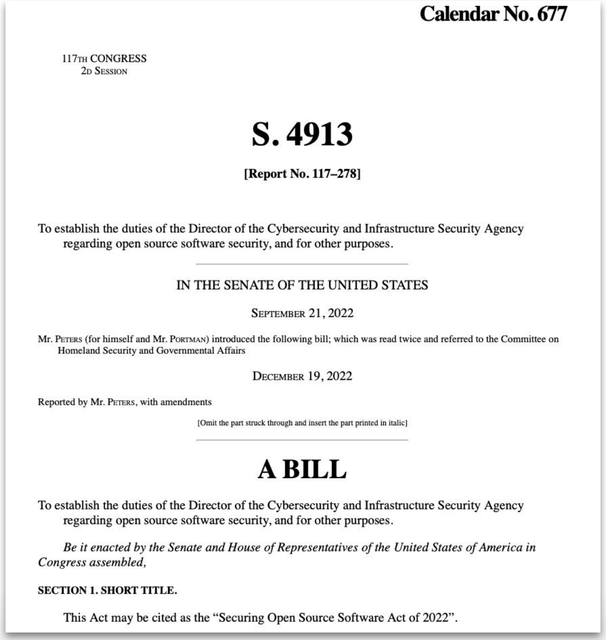
Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM ▸ PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

EU Cyber Resilience Act

For safer & more secure digital products



Calendar No. 677

117TH CONGRESS
2D SESSION

S. 4913

[Report No. 117–278]

To establish the duties of the Director of the Cybersecurity and Infrastructure Security Agency regarding open source software security, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 21, 2022

Mr. PETERS (for himself and Mr. PORTMAN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

DECEMBER 19, 2022

Reported by Mr. PETERS, with amendments

[Omit the part struck through and insert the part printed in italic]

A BILL

To establish the duties of the Director of the Cybersecurity and Infrastructure Security Agency regarding open source software security, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Securing Open Source Software Act of 2022".

US Strategy

*“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**.”*

NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

EU Cyber Resilience Act
For safer & more secure digital products
#DigitalEU #CyberSecEU

Background / Introduction

The European Commission has proposed a new legislation intended to improve the state of cybersecurity for software and hardware products made available in Europe.

- Draft legislation is now in the political process in the EU Parliament and Council

The initial draft of the Cyber Resilience Act (“CRA”) would:

- Improve the security of all products with digital elements made available in Europe
- Require that all manufacturers take security into account across both their development processes and the lifecycle of their products once in the hands of consumers
- Require that manufacturers apply the CE Mark to their products to indicate conformance to the requirements of the CRA

Additional Details

- Applies to all software whether embedded in cyber-physical systems, packaged software, or SaaS
- Process requirements:
    - Mandates the use of SBOMs, security patches, user ‘call home’ functionality
    - Requires support of products for no less than 5 years
    - Restricts publication of unfinished software for testing purposes
    - Imposes process and documentation requirements on a per-release basis
- CE Mark requirements:
    - Three tiers of product types, with increasing compliance obligations for ‘critical’ and ‘highly critical’ products
        - Critical and Highly Critical systems must use external audits for release certification

CE Mark Process for Software

Document
Fully document the development, release, and maintenance processes for each project in accordance with the CRA

Certify
Ensure that each project conforms to the processes and legally attest to conformance

Audit
Engage external CE Mark auditors for ‘critical products’ including operating systems

Each Release
For each release of software, repeat all of the above

Anyone making software available (*downloadable*) on the extended single market

Photo by Nicholas Ng on Unsplash

- Developers
- Providers of software
- Providers of digital services
- Online marketplaces & repositories

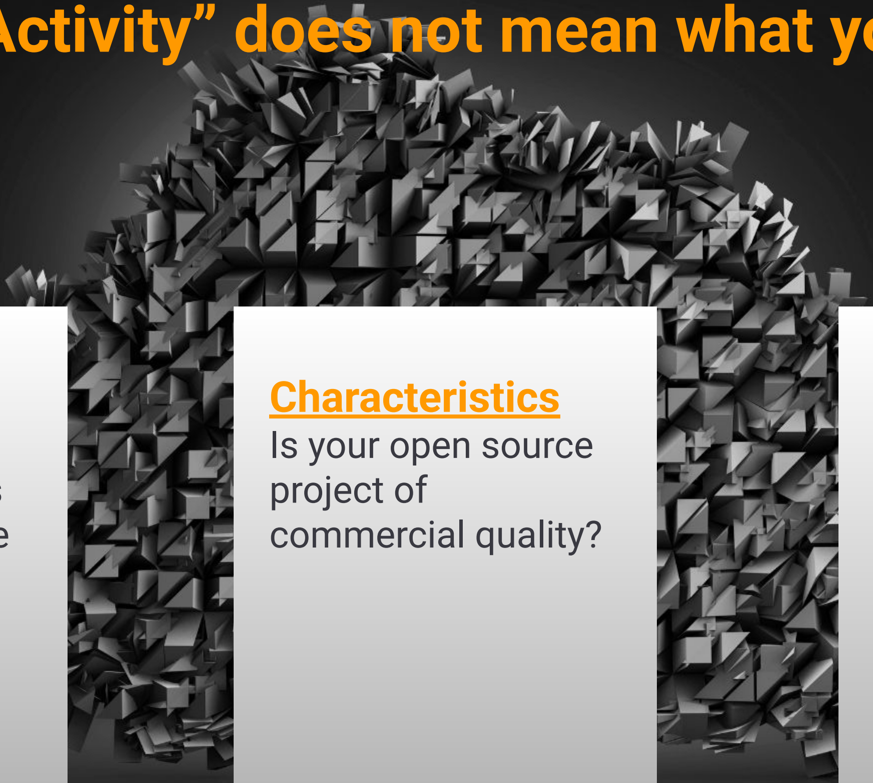
Photo by Kevin Limbri on Unsplash

Cyber Resilience Act and Open Source

Recital 10

> *In order not to hamper innovation or research, free and open-source software* ***developed or supplied outside the course of a commercial activity*** *should not be covered by this Regulation.*

“Commercial Activity” does not mean what you think it means



Regularity

Is there a regularity of supply? I.e. does your project release on a regular, repeated cadence?

Characteristics

Is your open source project of commercial quality?

Intentions

Do you intend for your open source project to be used in a commercial setting?

Cyber Resilience Act and Open Source

> **Recital 10**
>
> *In order not to hamper innovation or research, free and open-source software* ***developed or supplied outside the course of a commercial activity*** *should not be covered by this Regulation.*

Who does it exclude?

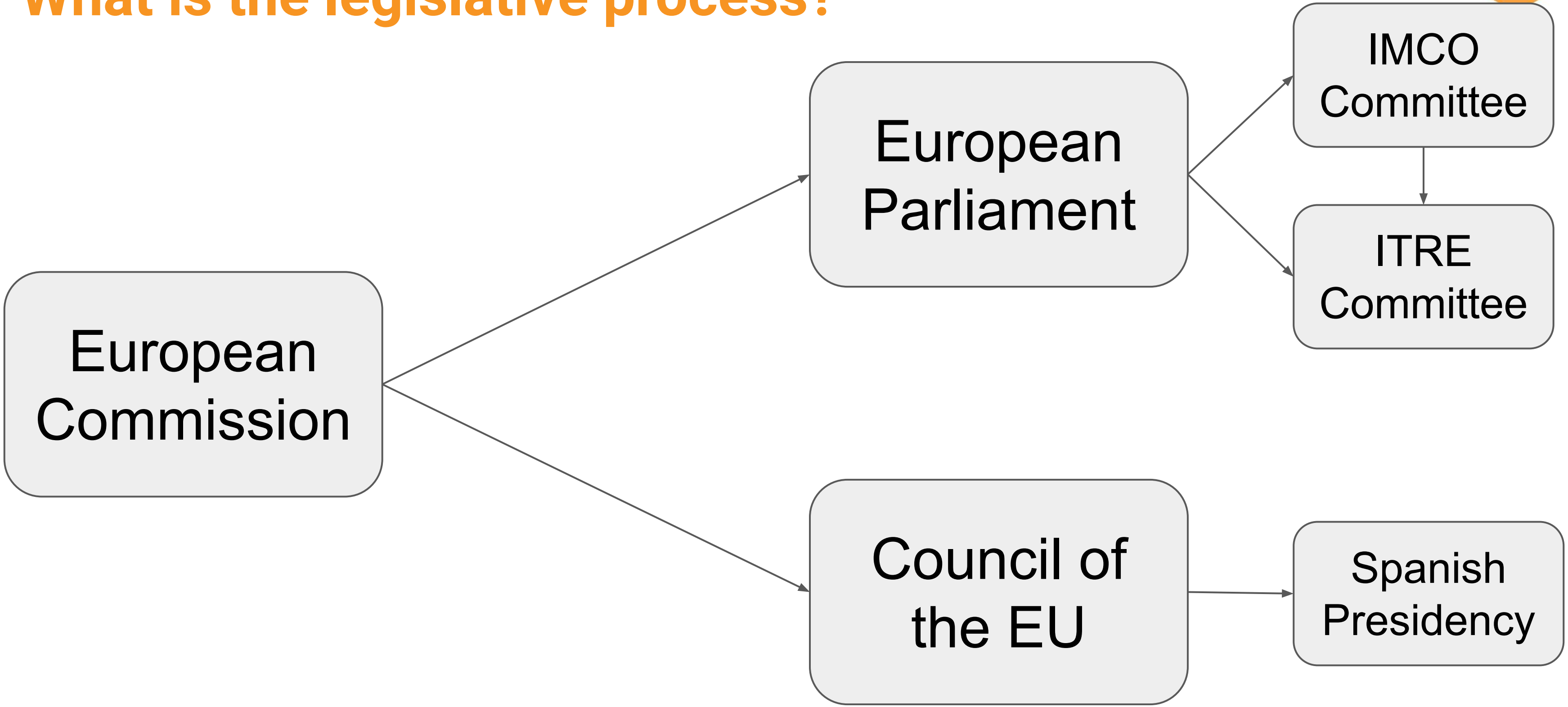
Hobbyists & Charities

Photo by Marius Ciocirlan on Unsplash

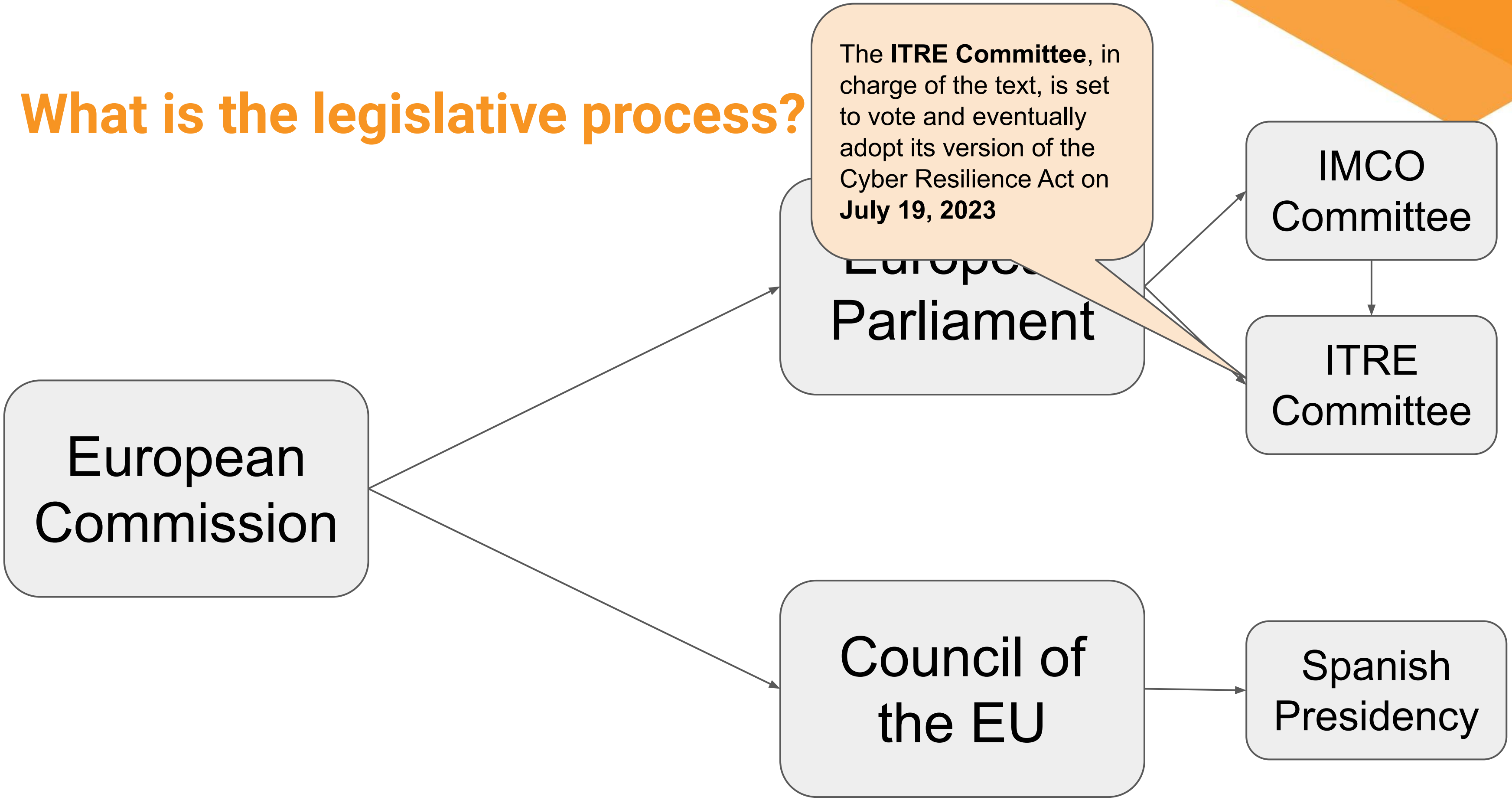
Penalties

The non-compliance with the essential cybersecurity requirements laid down in Annex I and the obligations set out in Articles 10 and 11 shall be subject to **administrative fines of up to 15 000 000 EUR** 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.

What is the legislative process?

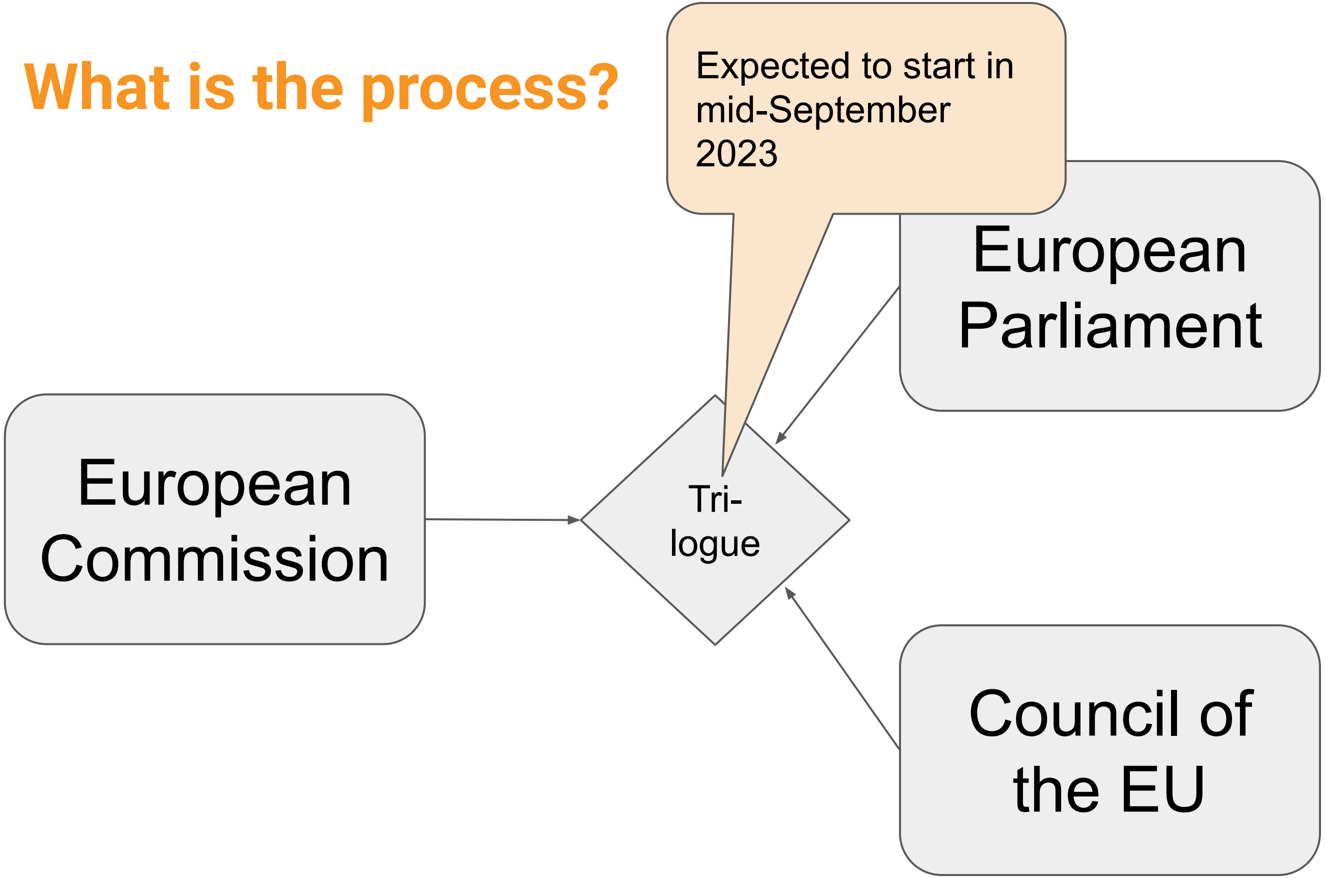


What is the legislative process?



The **ITRE Committee**, in charge of the text, is set to vote and eventually adopt its version of the Cyber Resilience Act on **July 19, 2023**

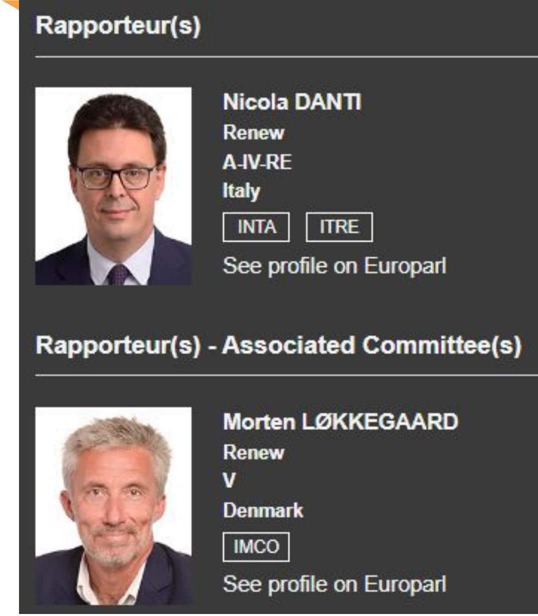
What is the process?



Expected to start in mid-September 2023

CRA: Current Status

- European Parliament ITRE (lead) and IMCO committees have drafted amendments
- The IMCO amendments seem positive for open source
- The discussions and drafted amendments of ITRE are very worrisome
- Commission remains adamant that open source must be regulated consistently as per the New Legislative Framework and Blue Guide, so outcome of trilogue is worrisome



Rapporteur(s)

Nicola DANTI
Renew
A-IV-RE
Italy
INTA ITRE
See profile on Europarl

Rapporteur(s) - Associated Committee(s)

Morten LØKKEGAARD
Renew
V
Denmark
IMCO
See profile on Europarl

CRA: Current Status

- The ITRE Committee has reached the firm conclusion: **most open source projects and all open source foundations should be responsible for CE Mark conformance**.
    - This is intentional.
    - This is not a misunderstanding.
- Their rationale:
    - Expensive for European SMEs to implement the CRA
    - Reduce the financial burden on the EU economy by putting OSS projects, OSS Foundations in charge of conformance
        - Assumes that CE Mark conformance is transitive

ITRE Draft: Problem 1

- Any open source project which has committers who are employed by a commercial entity will be deemed to be a commercial activity
- Why is this a problem?
  - This would encompass virtually every meaningful open source project on the planet
  - Set perverse incentives for struggling projects to reject people or contributions from the companies that use their software
  - Companies may ban their employees from participating in or contributing to open source projects

ITRE Draft: Problem 2

- Any project which accepts recurring donations from commercial entities will be deemed to be commercial
- Why is this a problem?
  - Open source sustainability is a serious problem
  - Projects will be incented to decline donations that could have otherwise been used to support their work

ITRE Draft: Problem 3

- Publication of intermediate builds, milestones, etc. must be restricted to a particular geographical area, limited in time, and with use restricted to testing only.
- Why is this a problem?
  - The publication of integration builds under open source licenses has been considered best practice for over 30 years. These are often made available indefinitely for regression testing purposes
  - This will essentially make open source development best practices prohibited

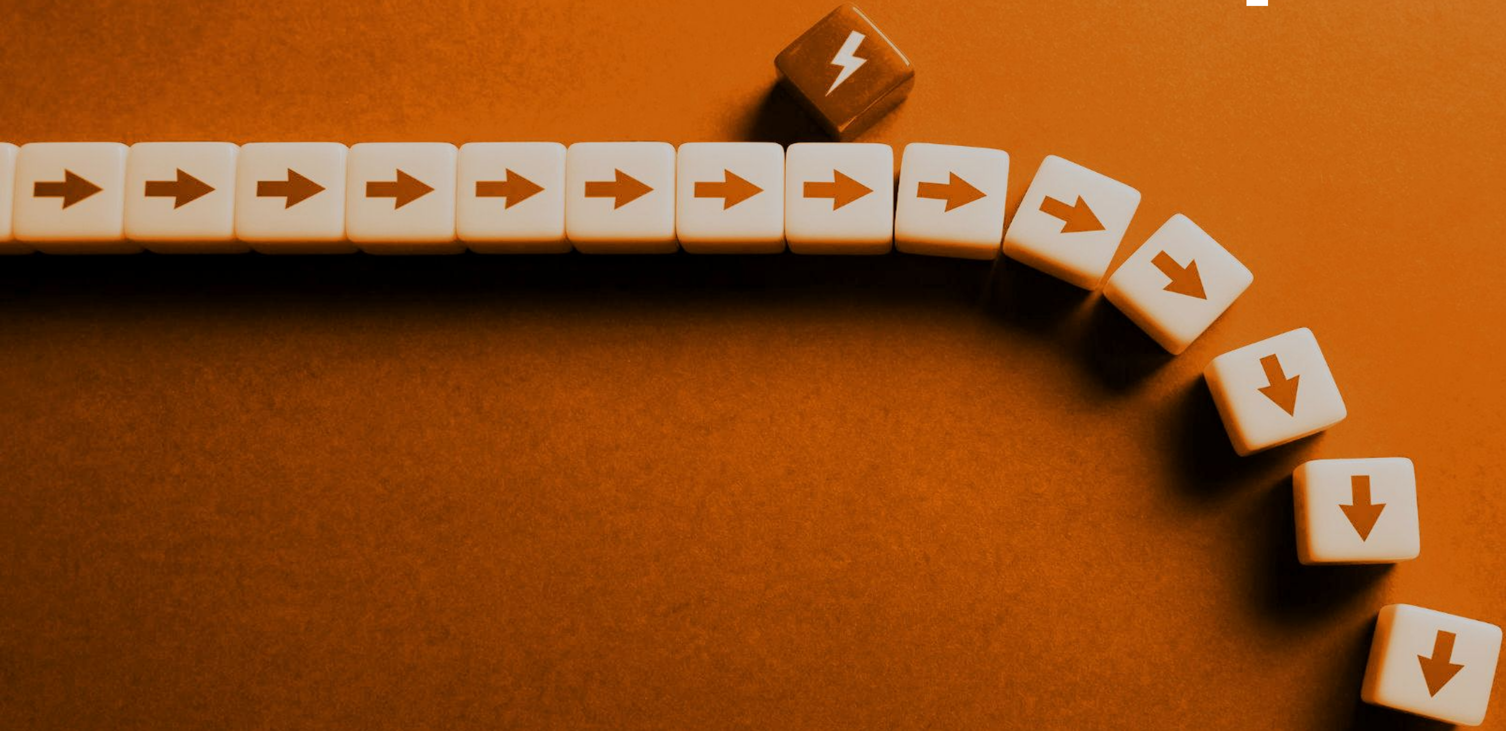
ITRE Draft: Problem 4

- All exploited vulnerabilities must be reported to ENISA within hours, regardless if a fix is available
- Why is this a problem?
  - Breaks accepted best practices for coordinated vulnerability disclosure
  - For unpatched vulnerabilities, runs counter to best practices to limit disclosures to only those able to contribute to the fix
  - Creating a central repository of unpatched vulnerabilities will not make software more secure
  - Creates a terrible precedent for other governments to follow

Council Drafts

- More positive news here, as generally open source projects and foundations would be excluded from “commercial activity”

Potential Consequences



Impact Assessment

In order to comply, projects, communities, and foundations will have to:

- Develop, document, and implement policies and procedures for every project, incl. all of the following:
  - development and post-release security requirements set forth in Annex I, including providing notification and update mechanisms.
  - user documentation requirements set forth in Annex II
  - product technical documentation set forth in Annex V
  - determine whether third party libraries used by each project are CRA compliant
- For each project release, prepare the project-specific documentation required by Annex V
- Determine for each project whether it meets the definition of ‘product with digital elements’, ‘critical product with digital elements’, or ‘highly critical product with digital elements’.
- For each single project release, document that the relevant CE mark process is followed...

We estimate that in any given year, EF’s projects alone make available several hundred releases.

Impact Assessment

CE Markings for Software Products

- Core objective of the proposed legislation is to extend the CE Mark regime to all products with digital elements sold in Europe
- Coupled with revisions to Product Liability Directive to extend to software products

Assumption:

- Process will be applied to OSS made available under OS licenses and provided free of charge, ostensibly under licenses which disclaim any liability or warranty.

Our Concern:

- CRA could fundamentally alter the social contract which underpins the entire open source ecosystem: open source software provided for free, for any purpose, which can be modified and further distributed for free, but without warranty or liability to the authors, contributors, or open source distributors.

Non-European producers of open source code don’t permit its use in Europe

A reasonable and rational response not to accept statutory responsibility obligations for something you **make available for free.**

Severing the EU’s access to Linux, Kubernetes, Apache, etc would cripple its innovation economy

European producers of open source will be at disadvantage relative to their international peers

Since they cannot avoid the responsibility obligations, they will be forced to accept them as part of their operations.

For some projects, it would probably be simpler to just terminate the project and pull its source code off of the internet.

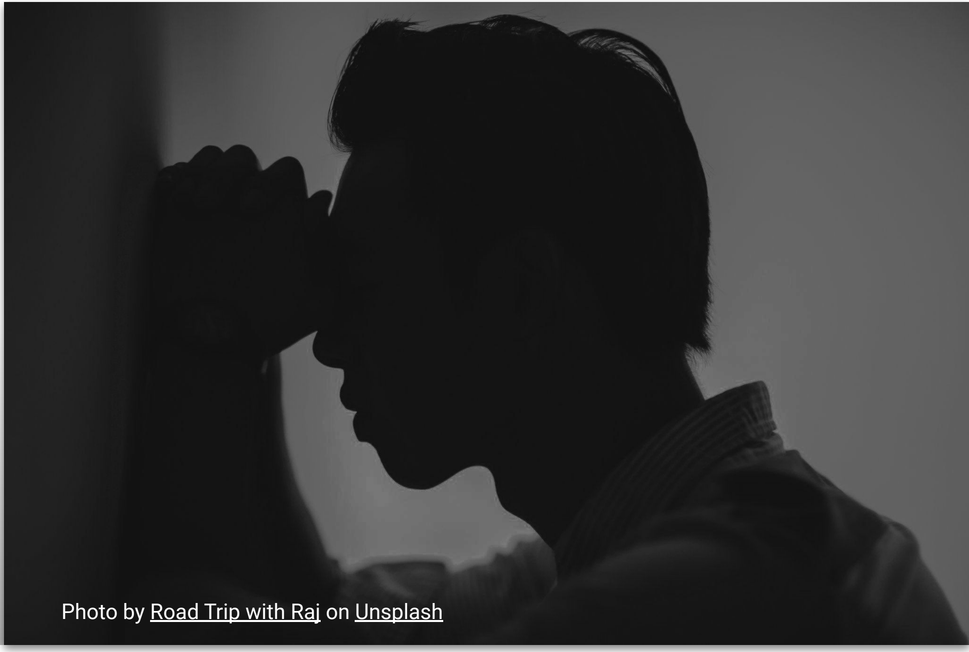


Photo by Road Trip with Raj on Unsplash

None of the package distribution sites are in a position to accept responsibility for the packages they make available

> “
>
> *…the consequence of this would be [Maven] Central, npm, PyPi and countless other repositories being **suddenly inaccessible to the European Union**.*
>
> *— Brian Fox of Maven Central, Sonatype*

Photo by [Handy Wicaksono](#) on [Unsplash](#)

Force European businesses to stop contributing to open source projects

At the moment, it is generally understood that **the risk** that contributions to open source may incur responsibility to the company **is low**.

The CRA changes that equation and as a result European companies may curtail their open source collaborations

➔ Extremely damaging to the innovation economy in Europe

➔ Runs counter to numerous European-wide strategies (digital sovereignty; GAIA-X, Catena-X, Dataspaces, Digital Twins, and Industrie 4.0)

Is this bad?

Photo by Japheth Mast on Unsplash

Call to Action

- Join us at OpenForum Europe
    - Multi-stakeholders discussions are happening there
    - Join the conversation at https://groups.google.com/a/openforumeurope.org/g/foss-community
- Publicly state your position that development of European open source is critical to Europe's prosperity and digital sovereignty and the limited role and ressources of foundations.
- Engage directly with the policy makers of your country (MEPs, governments) and corporate public affairs departments
    - Members of the ITRE Committee can be found via this page: https://www.europarl.europa.eu/committees/en/itre/home/members
- Educate your colleagues in government relations on the importance of open source to **your** business
    - Reach out to your public affairs or public policy department to ensure that this is understood and communicated about

Further Reading ...

- No cyber resilience without open source sustainability by Mike Linksvayer (Github)
- Open-source software vs. the proposed Cyber Resilience Act by Maarten Aertsen (NLNet Labs)
- The EU's Proposed Cyber Resilience Act Will Damage the Open Source Ecosystem by Olaf Kolkman (Internet Society)
- The Ultimate List of Reactions to the CRA by Simon Phipps (OSI)
- European Cyber Resiliency Act: Potential Impact on the Eclipse Foundation
- Cyber Resilience Act: Good Intentions and Unintended Consequences

ECLIPSE FOUNDATION

Thank you!

Questions?