GitHub

88 Colin P Kelly Jr Street
San Francisco, CA 94107
United States of America

January 23, 2023

**Making the Cyber Resilience Act work for open source software developers**

GitHub is the largest code repository and platform for collaborative software development. Home to over 94 million developers, and nearly 14 million in the EU, we are where the world builds software. GitHub welcomes the European Commission's efforts to improve cybersecurity in the single market and, in particular, the Cyber Resilience Act (CRA) proposal. We look forward to supporting the co-legislators as work on the CRA continues. Below we share several recommendations aimed at improving the CRA to help it achieve its aims while reflecting realities of software development practices, particularly for developers in the open source community.

Open source software is ubiquitous today, with 97 percent of code bases including open source components.[1] Open source software is often developed on a voluntary basis and individual project maintainers do not always have the same resources or dedicated security teams as the businesses that integrate their code into products. The open source community generates significant benefit for the EU—estimated at between €65 and €95 billion for the single market in 2018 alone[2]—and warrants careful support.

A primary challenge in cybersecurity within open source software is timely patching: while the open source community may promptly mitigate a vulnerability, downstream companies shipping products have historically been too slow to apply the fixes.[3] Open source licenses disclaim all warranty,[4] making explicit the expectation that any entity seeking to use or integrate the open source software bears responsibility to ensure its compliance with relevant laws. Entities selling products that integrate freely available open source software should be incentivized to ensure the security of the code they integrate and to maintain that security with timely patches. The CRA proposal takes important steps to achieve this aim, and it is encouraging to read the CRA proposal's Recital 10 that acknowledges the important role played by open source software. Our recommendations below improve upon this intent.

Further action should be considered to support open source in Europe. The model presented by the German Sovereign Tech Fund—where government resources are deployed to support developers maintaining open source

[1] Synopsys Open Source Security and Risk 2022 report.
[2] The Impact of Open Source Software and Hardware on Technological Independence, Competitiveness and Innovation in the EU Economy report.
[3] For example, the 2017 Equifax data breach, which saw sensitive data of nearly 150 million people leaked, followed from Equifax's failure to apply an available patch in a timely manner.
[4] For example, the European Union Public License (EUPL) and MIT License.

software projects of strategic importance—is worthy of careful study and possible emulation at the EU level. Government has historically played a central role in the provision of infrastructure, and it can support digital infrastructure by encouraging the open source software commons.

**Recommendation 1:**
**Improve clarity of Recital 10 exemption for open source**

Recital 10 of the CRA proposal is a helpful starting point to ensure that legislation seeking to improve cybersecurity of products does not unduly burden the open source community simply because companies make use of open source software in finished products. However, the scope of "commercial activity" is unclear and risks bringing into scope activities that are not placing a product on the market per se. We recommend offering explicit language in the Recital to clarify this, specifying "paid or monetised product" instead of "commercial activity."

Further clarification on services is warranted. NLnet Labs, for example, is a non-profit that builds open source software and offers paid support services. These support and consulting services related to open source software should be clarified as out of scope. As should general financial support for developers. GitHub Sponsors, one of many such programs, enables individuals and organizations to contribute money to individual open source developers and projects—not on a contract basis, but instead to enable them to focus on open source and potentially forgo other work. In both cases, services and general financial support do not change the fact that these open source projects and developers are not placing software onto the market as a paid product. Thus, we recommend that Recital 10 be re-written as:

> ***In order not to hamper innovation or research, free and open source software should not be covered by this Regulation unless it is offered as a paid or monetised product. This is in particular the case for software, including its source code and modified versions, that is openly shared and freely accessible, usable, modifiable and redistributable. Free and open source software development contributes between €65 billion to €95 billion to EU GDP annually according to research by the European Commission and depends on both volunteer and professional contributions from developers in independent, academic, enterprise, and government roles. In the context of software, a paid or monetised product might be characterized not only by charging a price for a product, but also by charging a price for subscriptions to software updates, by providing a software platform through which the manufacturer monetises other services, or by the use of personal data for reasons other than exclusively for improving the security, compatibility or***

> ***interoperability of the software. Technical support, consulting services, and financial sponsorships are not products within the scope of this Regulation.***

**Recommendation 2:**
**Exempt open source in Article text to improve certainty**

The intent of Recital 10 should be implemented with additional certainty by moving the open source software exemption into Article 2. Scope:

> ***This Regulation does not apply to free and open-source software, including its source code and modified versions, except when such software is provided as a paid or monetised product.***

**Recommendation 3:**
**Clarify the intended scope of "Distributor" with regards to software development platforms**

To support the secure development and patching of software products, the CRA should improve clarity of the "distributor" definition. In applying this New Legislative Framework concept to software, app stores and other means of distributing finished software products could be sensibly within scope. However, there is a risk that platforms that support the development of these software products may be brought within scope.

Code hosting and collaboration platforms, including GitHub and self-hosted servers belonging to individuals and organizations, support the development of software by enabling interested developers to obtain and contribute to source code and precompiled binaries. Package managers, including npm (which GitHub runs) and a large variety of others run by other companies, foundations, and communities, for programming languages (e.g., Cargo for Rust) and operating systems (e.g., Debian), support the development of software products by distributing binary components that can be integrated into numerous software products. Package managers and code hosting and collaboration platforms support the distribution of software under both open source and proprietary licenses. These actors serve important research and development functions distinct from distributors such as app stores which offer products without affecting their properties.

Defining distributors broadly could conflict with existing legislation. The Digital Services Act (DSA) provides conditional exemption of liability for hosting content, as does the Copyright Directive for open source software development and sharing platforms. The Commission's Product Liability Directive (PLD) proposal acknowledges the DSA exemption for online platforms, with guidance about applying the exemption under the PLD: "when online platforms do so present the product or otherwise enable the specific transaction, it should be possible to hold them liable, in the same way as distributors under this Directive. That means that they would be liable only when they do so present the product or otherwise enable the specific transaction, and only where the online platform fails to promptly identify a relevant economic operator based in the Union" (Recital 28). Similarly, the CRA should clarify the specific cases where online platforms do not enjoy liability exemptions.

### Recommendation 4:
### Clarify scope for software components not intended for end-use

The CRA proposal aims to improve the cybersecurity of products with digital elements placed on the market in the EU. The definition of "product with digital elements" may be currently read to include stand-alone software components. However, the CRA-outlined product-oriented security processes, labeling, documentation, and conformity assessment requirements may be poorly suited for components that are not intended as finished products for end-users.

We recommend that the CRA focus product requirements on software that is intended to be a product on the market. For example, the GitHub Enterprise Server, an on-premises software development application for business customers, would be considered a product whereas libgit2, a version control component, should not be considered a product, but instead a component for further integration, and therefore out of scope of product-specific requirements. Requirements for software components, as distinct from products, should be clarified within the CRA.

### Recommendation 5:
### Revise Annex I requirements to apply industry best practices

In addition to hosting an online platform for software developers, GitHub builds and ships software products. We encourage the Commission to incorporate industry best practices into the product requirements listed in Annex I. In particular, Annex I requires delivery "without any known exploitable vulnerabilities" but this risks an unobtainable objective, as manufacturers regularly learn of new vulnerabilities and make risk-based assessments on the need to prioritize fixes for timely delivery of product updates. In many cases, vulnerabilities may be identified that do not affect the security of a software product in practice because, for example, they may only be exploitable in environments where the product is not intended for use or they may not be reachable via any exposed API. We recommend removing this requirement from the Annex.

Similarly, the vulnerability handling requirements outlined in Annex I raise concerns. In particular, the requirement to “remediate vulnerabilities without delay” may undermine established practices of coordinated vulnerability disclosure and risk-based assessments from manufacturers on when to push and how to coordinate security updates. Vulnerabilities exist on a continuum of risk, and risk-based prioritization means that in practice software production does not necessarily cease whenever a vulnerability is discovered. We recommend striking “without delay” or otherwise qualifying this requirement to align with coordinated vulnerability disclosure practices.

. . .

As European policymakers consider regulations that apply to software development, it is essential that they consult developers. Developers have intimate knowledge of current industry processes, pioneer security best practices, and understand the importance of open source. They work in organizations and roles throughout the economy and for European institutions, including the Commission’s Open Source Program Office. They also engage in technical and policy organizations, including the Open Source Security Foundation and OpenForum Europe. As the Cyber Resilience Act moves forward, we encourage all policymakers to seek out developers’ perspectives.

At GitHub, we believe that the health of the developer community is critical to the security of all software. As the home to the world's largest developer community, GitHub is uniquely positioned and committed to helping developers advance the security of their code, and we take this responsibility seriously. We look forward to working with the European Commission, Council, and Parliament to advance this mission in the Cyber Resilience Act and beyond.