RIPE NCC
RIPE NETWORK COORDINATION CENTRE

To: ITRE's (shadow) rapporteurs on the Cyber Resilience Act

Amsterdam, 21 April 2023

Dear Members of the European Parliament,

As the Regional Internet Registry for Europe, the Middle East and parts of Central Asia, the RIPE NCC welcomes the European Commission's efforts to further harmonise and improve cybersecurity in the European Union by setting essential cybersecurity requirements for all products with digital elements that are placed on the EU market. We therefore support the proposed Cyber Resilience Acts's (CRA) cybersecurity-by-design approach, as well as the included obligation for manufacturers and other relevant operators to provide end users with clear and understandable information about their products with digital elements. Manufacturers, distributors and other relevant operators can benefit from the legal clarity and certainty created by avoiding fragmentation on the topic between different Member States within the EU's single market.

The RIPE NCC would like to use this opportunity to reiterate[1] the RIPE community's concerns regarding the limited exemption, formulated in Recital 10 of the CRA, for the development and making available of open-source software. We do so in our role as secretariat for RIPE, which is an open, inclusive community that welcomes the participation of anyone with an interest in IP-based networking. We also do so as an organisation that publishes the source code for several of its own products/services, under various public licences, via repositories such as GitHub. This is something we do, not with the intention to make the software available as an independent product for end users, but for transparency and research purposes, outside our standard business context/activities as a Regional Internet Registry.

As we highlighted in our response to the European Commission's proposal, open-source software is often published by one developer and then built upon and modified by many others, some of whom may ultimately incorporate it into a product to be placed on the market. In this sense, there is often not a clear-cut distinction of who can be considered the "manufacturer". As open source veteran and expert Simon Phipps has said, 'Open source is an artefact arising from the interactions of a community of contributors with no contractual binding between them beyond the open source licence itself, which disclaims all warranties and has no conduit for funds'[2].

For the CRA to reach the goal of reducing product vulnerability, it also needs to reduce vulnerability in open-source software — an aim the RIPE NCC strongly supports. The lack of clarity surrounding the notion of "commercial activity" referred to in Recital 10 however, is what creates uncertainty for, and risks placing undue regulatory burden on, those from the community who contribute to open-source software and its security without the intent of making a profit as a result of its later use. The Blue Guide does not give sufficient clarity as to when open-source

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13410-Cyber-resilience-act-new-cybersecurity-rules-for-digital-products-and-ancillary-services/F3376593_en
[2] https://the.webm.ink/open-source-is-conceptually-disjoint-from-proprietary-software

Registered in Amsterdam Chamber of Commerce No. 40539632
Bank ABN-Amro EUR Account No. NL 37ABNA0618139087
VAT No. NL806268220B01

Stationsplein 11
P.O. Box 10096
1001 EB Amsterdam
The Netherlands

T: +31 20 535 4444
F: +31 20 535 4445
E: ncc@ripe.net
W: www.ripe.net

software is considered to be developed or supplied in the course of a commercial activity[3]. We therefore urge ITRE / IMCO to provide a clearer definition of what constitutes open-source software that is not within the scope of the proposed CRA.

To that end, we suggest including the following in Recital 10, the text in bold, from the Council's Presidency compromise proposal dated 10 March 2023:

- The supply in the course of a commercial activity might be characterised not only by charging a price for a product, but also by charging a price for technical support services ***when this does not serve only the recuperation of actual costs or pursues a profit or the intention to monetise***, by providing a software platform through which the manufacturer monetises other services, or by requiring as a condition for use, the processing of personal data for reasons other than exclusively for improving the security, compatibility or interoperability of the software. ***The circumstances under which the product has been developed, or how the development has been financed should not be taken into account when determining the commercial or non-commercial nature of that activity.***

Adding this change to recital 10 helps provide the required clarity as to what falls within the course of a commercial activity when it comes to open-source software.

Respectfully,

The RIPE NCC

[3] See 2.2 of https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C:2022:247:FULL&from=EN
'Commercial activity is understood as providing goods in a business related context. Non-profit organisations may be considered as carrying out commercial activities if they operate in such a context. This can only be appreciated on a case-by-case basis taking into account the regularity of the supplies, the characteristics of the product, the intentions of the supplier, etc. In principle, occasional supplies by charities or hobbyists should not be considered as taking place in a business related context.'

Stationsplein 11
P.O. Box 10096
1001 EB Amsterdam
The Netherlands

T: +31 20 535 4444
F: +31 20 535 4445
E: ncc@ripe.net
W: www.ripe.net