Joint Statement: Strengthening Open Source Sustainability via Article 25 of the EU Cyber Resilience Act

Our Core Position

> *We believe the voluntary attestation framework, described in Article 25 of the CRA, offers a transformative opportunity to strengthen open source sustainability. By creating a mechanism to standardise and formally recognise security information provided by open source projects, the overall compliance burden can be reduced and projects can become more attractive to manufacturers by making it easier to carry out their due diligence obligations. We believe Article 25 can enable sustainable long-term funding, and bolster community-led self-governance of open source projects, improving cybersecurity across the European market, and lowering the compliance burden that the CRA would otherwise impose on small and medium enterprises.*

The four pillars of our proposed Article 25 Framework

1. Facilitating efficient Due Diligence via trusted artefacts. The CRA requires manufacturers to perform due diligence on every integrated component, including free and open source components. We support the development of interoperable, open standards for attestation artefacts that can eliminate the "denial-of-service attack" on maintainers caused by duplicative compliance requests and provide manufacturers with consistent, trustworthy information they can integrate into their risk assessments, and that can also be accessible by the Market Surveillance Authorities.

2. Incentivising security maintenance across the supply chain. Attestations create a bridge between regulatory requirements and economic support. This framework provides a structured pathway for manufacturers to financially support the investment in ongoing security made by the stewards and maintainers of projects they use and rely on, that goes directly and transparently to each open source project

3. Strengthening community-led governance and resilience. We advocate for an attestation model that is strictly voluntary, adaptable to the open source project, and risk-based, ensuring there are different levels of attestation so that projects can choose the level that matches their interests and capacity. The framework must avoid indirect compliance pressure on micro-projects and independent maintainers. Proportionality is essential to preserve the diversity and decentralised nature of open source ecosystems.

4. Safeguarding openness and market neutrality. The voluntary attestation framework ensures market neutrality and prevents undue burdens by remaining strictly voluntary and non-discriminatory. It should offer free, baseline artifacts as the default for maintainers. Choosing not to provide higher-tier attestations does not imply non-compliance, as manufacturers remain ultimately liable for their own risk assessments. This approach protects diverse governance models across all project sizes.

Conclusion

Voluntary Security Attestations are not a “proposal” of the open source community, they are an option explicitly mentioned in the European law, and represent a unique opportunity for the European Commission to facilitate due diligence obligations of manufacturers while empowering open source communities. Voluntary attestations should also support the role of Member State market surveillance authorities under the CRA. Where appropriate, alignment with the EU cybersecurity certification framework and guidance from the European Union Agency for Cybersecurity (ENISA) would enhance coherence and legal certainty.

While the details of the potential Delegated Act on attestations are not yet available, we look forward to continuing to collaborate with the open source community and with the European Commission, and to clarify and operationalise manufacturer accountability in a proportionate manner.