Brussels, 6 November 2023

SUBJECT: The Cyber Resilience Act as it stands risks creating COVID-style supply chain disruptions

Dear Vice-President Schinas, Vice-President Jourová, Commissioner Breton, Secretary of State Carme Artigas, Nicola Danti MEP,

On behalf of DIGITALEUROPE, we are writing to you to express our concerns about the current negotiations towards a Cyber Resilience Act (CRA) and offer our solutions as we enter this crucial final phase of negotiations.

As you know, we have long been supportive of horizontal cybersecurity rules for connected products rather than a patchwork of different rules per sector. However, **the law as it stands risks creating bottlenecks that will disrupt the single market, affecting millions of products– from washing machines to toys, cybersecurity products, as well as vital components for heat pumps, cooling machines and high-tech manufacturing**.

Given the CRA's wide scope and a lack of capacity, **we face a situation where secure products cannot be placed on the market and will be blocked for EU customers**. Europe cannot currently offer so many conformity assessments, creating bottlenecks as manufacturers must prove compliance through third party certifiers for products listed in Annex III. This will have a huge effect on the wider supply chains, as many of these components are crucial inputs for the European economy and the green transition. **We risk creating a COVID-style blockage in European supply chains, disrupting the Single Market and harming our competitiveness**.

To fix this, we propose the following amendments:

1. **Maximise the possibility of self-assessment**, like we have seen in the AI Act.
2. **An implementation period of a minimum of 48 months** to allow for the development of harmonised standards.
3. **Significantly reduce the list of higher risk products in Annex III,** as in the Council's position.

A second group of concerns relates to **reporting.** Back in June, together with a broad group of industry groups we raised the alarm on the dangers of reporting unpatched vulnerabilities, concerns also echoed by civil society and security experts. In addition, we are concerned that the volume of reporting will be too high for public authorities to handle, given the 300,000 gap[1] in cybersecurity specialists in Europe.

If co-legislators insist on maintaining actively exploited vulnerabilities in scope, we ask for some key safeguards:

1. **Manufacturers should be allowed to make a judgement call to prioritise patching over immediate reporting based on justified cybersecurity-related grounds**. For example, if reporting the unpatched vulnerability risks the malicious software spreading

[1] ENISA, Addressing Skills Shortage and Gap Through Higher Education, 2021

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

further. Not every case is the same. In practice, this could be reflected by amending the Council's proposed Art. 11(1) – please see our suggestion in the annex.

2. As in NIS2, **reporting should be limited to incidents and vulnerabilities that pose a significant cybersecurity risk**. To avoid duplication of efforts we also urge for the respect of the "**one incident-one report**" principle.
3. Additionally, **we support the Parliament's definition of an 'actively exploited vulnerability'**, whereby there must be reliable evidence of a successful hack, rather than just an attempt, and the clarification that vulnerabilities discovered with no malicious intent should not be subject to mandatory notifications.

Yours sincerely,

Cecilia Bonefeld-Dahl, Director General of DIGITALEUROPE

Dr. Roland Busch, President and CEO of Siemens AG

Börje Ekholm, President and CEO of Ericsson

Dr. Stefan Hartung, Chairman of the board of management of Robert Bosch GmbH

Peter Herweck, CEO of Schneider Electric

Pekka Lundmark, President and CEO of Nokia

Richard Marko, CEO of ESET

Annex:

Our proposed change to Article 11 (1)

The manufacturer shall, ~~without undue delay and in any event within 24 hours~~ after becoming aware of it, notify **to TBD** any actively exploited vulnerability **that poses a significant cybersecurity risk,** contained in the product with digital elements. The notification shall include details concerning that vulnerability and, where applicable, any corrective or mitigating measures taken.

Only in case co-legislators insist on keeping reporting of unpatched vulnerabilities in scope, the following should be included:

In exceptional circumstances and, in particular, upon request by the manufacturer and in light of the level of sensitivity of the information that would have to be notified by the manufacturer under paragraph 1, the notification may be delayed based on justified cybersecurity related grounds provided by the manufacturer for a period of time that is strictly necessary, where there is an ongoing process of developing a mitigation measure, including in cases where a vulnerability is subject to a coordinated vulnerability disclosure procedure as referred to in Article 12(1) of Directive (EU) 2022/2555.

About DIGITALEUROPE

DIGITALEUROPE is the leading trade association representing digitally transforming industries in Europe. We stand for a regulatory environment that enables European businesses and citizens to prosper from digital technologies. We wish Europe to grow, attract, and sustain the world’s best digital talents and technology companies. Together with our members, we shape the industry policy positions on all relevant legislative matters and contribute to the development and implementation of relevant EU policies, as well as international policies that have an impact on Europe's digital economy. Our membership represents over 45,000 businesses who operate and invest in Europe. It includes 105 corporations which are global leaders in their field of activity, as well as 41 national trade associations from across Europe.