Joint Statement on Cyber Resilience Act: Manufacturers of long-lasting industrial products

28 November 2023

We fully support the ultimate objective of the Cyber Resilience Act, which aims to cyber-protect the products and increase their cyber-resilience. It is of utmost importance to have effective processes for vulnerability management and handling, enabling manufacturers to promptly address security weaknesses.

Nevertheless, we, a diverse coalition of European associations representing various sectors, that manufacture long life-cycle products in industrial contexts (B2B) and long-manufacturing processes, **express our concerns regarding Article 10, Annex 1, Article 16, and Article 57 of the Cyber Resilience Act (CRA)**.

Indeed, the applicability of these provisions, especially in sectors characterised by long product life cycles, such as **rail products, construction machinery, and machine tools designed to last over 30 years**, poses significant challenges.

First, there is an inherent difficulty in accurately quantifying and estimating the efforts required to ensure the cyber resilience of complex products over such extended durations which raises doubts about the practicality of these obligations. Yet, what is certain is that this will represent a huge economic burden.

Secondly, a fundamental reality for our sectors remains that once a product is delivered, its future evolution, potential upgrades, and modernisation depend on the B2B end-user. Users will modify the product configuration after the warranty period without the involvement of the manufacturer, hindering meaningful vulnerability monitoring.

The cyber-resilience of digital products in B2B sectors will be achieved only through a balanced allocation of responsibilities between manufacturers and users.

As a result, **we advocate for a nuanced approach, aligning the final text with or even going further than the Parliament compromise text that emphasises differentiation between business-to-business (B2B) and business-to-consumer (B2C) context**.

We acknowledge the progress made in trilogues with the agreement reached during negotiations on the support period (Article 10(6)), with manufacturers being tasked to define its duration taking into consideration the time the product is expected to be in use, reasonable users' expectations, the nature of the product, its intended purpose and relevant Union law for a five-year minimum timeframe.

In Annex I, Section 2, Point 8, the specification allowing for contractual agreements between parties in a B2B context, particularly regarding the free transmission of security patches, is crucial for sectors

like rail, construction machinery, and machine tools. This provision recognises the unique dynamics of B2B relationships, fostering flexibility and cooperation between manufacturers and end-users.

Additionally, we emphasise the importance of Article 16 on substantial modifications and believe that clear guidelines defining what constitutes a substantial modification are paramount for the effective implementation of Article 16. **As product compliance with both CRA, Machinery Regulation and any other relevant regulation will be mandatory in the near future, consistency among different pieces of legislation applicable to the same products is key**, especially in terms of definitions and criteria establishing whether or not a modification is substantial.

Finally, due to the long manufacturing processes of complex products in the rail transport, construction machinery, and machine tools sectors, as underlined above, **we call on co-legislators to extend the transition period to at least 48 months in order to be prepared for the significant changes that the Cyber Resilience Act will bring to our industries.** This will minimise the disruption to ongoing projects that will lead to products being placed on the market in the years to come.

While we acknowledge the necessity of enhancing cyber resilience, **we urge the European Commission, European Parliament, and Council to consider the specific challenges faced by sectors with extended product life cycles and complex, long manufacturing processes.** We stand ready to collaborate with relevant stakeholders to provide insights and perspectives, ensuring that cyber vulnerabilities are addressed responsibly to safeguard the interests of both manufacturers and end-users across various industries.

Yours sincerely,

Riccardo Viaggi, Secretary General

CECE – Committee for European Construction Equipment, www.cece.eu

Filip Geerts, Director General

CECIMO – European Association of Manufacturing Technologies, www.cecimo.eu

Philippe Citroën, Director General

UNIFE – The European Rail Supply Industry Association – www.unife.org