STATEMENT

Brussels, 7 November 2023

Cyber Resilience Act: Europe's technology industries ask decision-makers to proceed with care and caution

We welcome the ambition of the European institutions to increase the level of cybersecurity in the European market. We also welcome the ongoing and continued consultation of stakeholders throughout the legislative process of the Cyber Resilience Act (CRA).

As the Regulation is in the process of being finalised in interinstitutional negotiations (trilogues), we urge the European institutions to take the time necessary to effectively address the remaining concerns of the industrial sector, avoiding at all costs the rushing through of this crucial piece of legislation on cybersecurity. We therefore encourage the European institutions to consider these five priority aspects in the next trilogue meetings:

1. Applicability timeline (Article 57 and transitional provisions in Article 55)

The co-signatories of this statement recognise the efforts made by the Council of the European Union (Council) and the European Parliament (EP) to extend the timeline for implementation of the CRA to 36 months.

However, we believe that an implementation timeline of 48 months is more suitable, especially in view of the time needed to develop harmonised standards for Class I products[1]. In addition, a staggered approach should be considered, which allows for an additional 24 months for the specificities of complex products such as Non-Road Mobile Machinery (NRMM).

[1] For additional information on why extended transition periods are necessary, please refer to Orgalim's position paper on "Enhancing EU manufacturing competitiveness with a future-proof approach to placing products on the Single Market"

Orgalim represents Europe's technology industries, comprised of 770,000 innovative companies spanning the mechanical engineering, electrical engineering, electronics, ICT and metal technology branches. Together they represent the EU's largest manufacturing sector, generating annual turnover of over €2,906 billion, manufacturing one-third of all European exports and providing 11.19 million direct jobs. Orgalim is registered under the European Union Transparency Register – ID number: 20210641335-88.

Orgalim aisbl
BluePoint Brussels
Boulevard A Reyers 80
B1030 | Brussels | Belgium

+32 2 206 68 83
secretariat@orgalim.eu
www.orgalim.eu
VAT BE 0414 341 438

2. Critical products classification methodology (Article 6 and Annex III)

We appreciate and support the changes made by the Council to the classification methodology in Article 6, as these propositions and clarifications prioritise criteria centred on cybersecurity and associated risks, primarily concerning functions critical to the cybersecurity of other products. The clarification of methodology in Article 6, and the subsequent modification of Annex III, answers several concerns of European industry, as it addresses the following:

i. A systemic approach to risk management and identification, taking into consideration the environment in which the product is used, as well as the cybersecurity functionality of the product.
ii. The use of international standards methodologies (such as IEC 62443) to self-assess against the essential requirements of the CRA.
iii. A reduction of the delay for entry into the European Union's market of products with digital elements, by reducing the bottleneck at the third party assessment stage.
iv. A reduction of the financial burden of compliance, linked to third party assessment.

To ensure the competitiveness of industrial manufacturers and an efficient implementation of the CRA by all stakeholders (including SMEs), we strongly support Article 6 as proposed by the Council.

3. Scope (Article 2)

3.1. Exclusion of spare parts

We support the exclusion of spare parts as proposed by the EP and the Council. This exclusion is important to ensure that the long-term investment of European industrial stakeholders is protected through the possibility of maintaining equipment and systems.

The co-signatories therefore urge that the exclusion of spare parts should be confirmed in the final text of the CRA.

3.2. Exclusion of free and open-source software (FOSS) development

A direct exclusion of FOSS development in the final text is important for innovation and should move the CRA responsibilities to the use of FOSS regarding a monetised product, and not to the provider of FOSS.

4. Manufacturers should be able to transparently determine a support period for the product (European Parliament's Article 10 (6))

We strongly support the EP's proposal for a support period that "*is proportionate to the expected product lifetime*". In light of the variety of hardware and software products under the scope of the CRA, manufacturers require some flexibility, especially considering the different composition of products with regard to their digital elements.

5. Sharpen the focus of the essential cybersecurity requirements (Annex I)

5.1. Specify the essential product requirement regarding known exploitable vulnerabilities

We support the approach of the Council to take the Annex I requirement (aa) regarding known exploitable vulnerabilities under the threshold of the risk assessment, and to further specify it by defining exploitable vulnerabilities in Article 3(38a).

5.2. Data minimisation principle

We urge regulators to limit the data minimisation principle to only "*personal data*", without widening the scope by making a reference to "*other*" data. While we recognise the need to include personal data, the extension to non-personal data would be disproportionate and unnecessary as non-personal data does not require the same level of protection as personal data. Moreover, the extension to non-personal data could hinder innovation and would lead to uncertainty regarding the interpretation and assessment of this requirement. We strongly recommend taking into account the specificities of the industrial sector in the tailoring of the essential requirements.

5.3. Differences in B2C and B2B also have to be considered in the essential requirements

For industrial and B2B settings, the obligation to disseminate and to make security updates available free of charge might not be appropriate in view of the criticality and complexity of industrial systems and installations. Therefore, we again urge legislators to take into account the specificities of the industrial sector in the tailoring of the essential requirements.

We call on the European institutions to address the above-mentioned issues by providing a clear and workable path to the industry, in order to ensure the efficient application of the CRA. We stand ready to engage in further discussions regarding our outlined concerns.

Yours sincerely,

orgalim
EUROPE'S TECHNOLOGY INDUSTRIES

And its member organisations:

CECE
COMMITTEE FOR EUROPEAN CONSTRUCTION EQUIPMENT

CEMA
European Agricultural Machinery Association

EGMF
European Garden Machinery Federation

euralarm
for a safer and more secure Europe

FEM
European Materials Handling Federation