



POSITION PAPER

Brussels – 21/02/2023

CECE comments on the Cyber Resilience Act proposal

Introduction

CECE, the Committee for European Construction Equipment, welcomes the European Commission's proposal, known as the Cyber Resilience Act (CRA), for a regulation on horizontal cybersecurity requirements for products with digital elements. CECE wishes to stress that, even today, the construction equipment sector is already committed to assessing the level of cybersecurity risk of connected digital products. Hence, original equipment manufacturers are already addressing cybersecurity risks not only by complying with existing requirements, but also by meeting customers' needs to protect their reputation.

In accordance with the legislation on product safety requirements, construction equipment manufacturers are attentive to ensure an adequate level of cyber resilience of their connected digital products with a view to matching customers' expectations on products' security. The risk of cybersecurity incidents has increased over recent years, as it evolves along with the multiplication of connected products on the market and technological changes. Nonetheless, the general awareness of cyber threats has also risen considerably in our industry, even though the number of cyber-attacks targeting our products remains limited. Overall, this has helped manufacturers to better address cyber threats by putting in place appropriate countermeasures.

With regards to the legislative proposal, CECE is concerned about the in-scope products and perceives timeframe-related issues in consideration of the proposed transition period, the availability of harmonized standards, the time needed for manufacturers to adapt to the new requirements and the accreditation of notified bodies. These points are explained in more detail below.

1. The scope is too broad and needs clarification

The construction machinery industry is concerned by the current wording of Article 2: the definition of in-scope products is too broad and leaves room for interpretation. We believe that the CRA should apply only to **connected digital products able to communicate data directly or indirectly via a publicly available electronic communications service within the meaning of Article 2(4) of Directive (EU) 2018/1972**. As such, we ask for the proposed definition of connected digital products to be reflected in the text of Article 2(1) and Article 3(1) of the CRA.

Furthermore, we ask for clarification regarding machinery products embedding connected digital products listed in Annex III. CECE represents manufacturers producing construction mobile machinery, including connected digital products that may be installed either by the machine manufacturer or by the user as aftermarket solutions. To maintain a well-functioning internal market and to avoid unnecessary double assessment and/or certification, we endorse the approach that **a default category product embedding a compliant critical product (listed in Annex III) is not considered a critical product itself** as per recital 27. As such, we call for this to be clearly stated in the binding provisions of the CRA with a view to ensuring legal certainty on the applicable conformity assessment procedures. This will clarify the construction machinery and component manufacturers' roles with regards to their obligations under the CRA.

CECE recommends that connected digital products placed on the market before the CRA application date together with their related **spare parts** are excluded from the CRA scope, even if the latter are placed on the market after the CRA applies.

Our industry also believes further clarification is needed on the applicability of the vulnerability handling requirements listed in Annex I.2 throughout the product lifecycle or for a period of 5 years: we suggest specifying in the binding part of the proposed regulation that **Annex I.2 requirements only apply to connected digital products placed on the market after the date of application of the CRA.**

2. Timeframe-related issues

Harmonised standards development

CECE questions **the announced timeframe for the delegated act, referred to in Article 6(3) of the CRA proposal, the adoption of which will take place after the entry into force of the CRA.** Given that the delegated act aims at *"specifying the definitions of the product categories under class I and class II as set out in Annex III"*, **we call on co-legislators to already consider including those definitions in the legal text of the CRA throughout the co-decision process.** In the absence of the definitions concerned, room for interpretation will remain until the publication of the delegated act, thus also hindering the standardisation work.

We understand from the tentative timeline announced by the European Commission that the CRA will have a 24-month transition period ending on the foreseen publication date of the harmonised standards by the European Standardisation Organisations (ESOs). As explained above, **the adoption of the delegated act clarifying the content of Annex III (expected within 12 months from the entry into force of the CRA) is likely to delay standardisation activities accordingly and hamper the smooth development of such standards.**

Furthermore, we would like to stress that the harmonised standards developed for the Delegated Regulation (EU) 2022/30 to the RED will likely need adaptation after the publication of the CRA to cover the broader requirements included therein, to eventually be listed in the OJEU and thereby provide presumption of conformity.

Implementation timeframe

Considering (a) the practical timeframe needed for the development of harmonized standards, (b) the recruitment of cybersecurity HAS consultants and the time to assess hundreds of harmonised standards, (c) the recurring delays for their citation in the OJEU, and (d) the fact that manufacturers need sufficient time to

implement the necessary design and process changes, **construction equipment manufacturers ask for a longer transition period of 5 years after the entry into force of the CRA.**

We are concerned that the timeframe foreseen under the CRA proposal is not sufficient for the implementation of the full set of essential requirements listed in Annex I. Combined with the essential health and safety requirements proposed under the upcoming Machinery Regulation, construction machinery manufacturers will be required to perform significant design changes to the current hardware and software architecture of their products in a short period of time. Therefore, CECE stresses the need for a sufficient implementation timeframe to allow the industry to update the whole product system and comply with the CRA requirements given the complexity of construction machinery products.

Availability of notified bodies

Finally, **in the absence of harmonised standards and where third-party assessment is required**, the lack of cybersecurity experts will represent a challenge to ensure that enough accredited notified bodies for cybersecurity will be readily in place to face the expected rush by manufacturers of all sectors once the CRA applies. This will become a serious obstacle to get the certificates in time for the planned placing on the market for manufacturers in need for such conformity assessment procedures.

Additional remarks

In addition to the key issues identified above, our industry calls for further consideration of the following:

- Regarding the schemes to be developed under the (EU) 2019/881 Cybersecurity Act (CSA) and the common specifications to be adopted by the European Commission, we reject that these measures could be acceptable alternatives to harmonised standards since they are not developed under the same transparency and consensus principles. In any case, no applicable schemes for our industry will be available in time.
- On the Annex I.1 product properties-related requirements, we ask for clarification on “(2) *Products with digital elements shall be delivered without any known exploitable vulnerabilities*”. CECE firmly believes that, in its current formulation, this requirement will significantly hinder the availability of products along the supply-chain. We do not recognise the term “deliver” as language of the NLF and suggest replacing it by concepts like “put into service” or “placed on the market”. Besides, we understand the reference to *known exploitable vulnerabilities* targets a list of common vulnerabilities presenting a substantial risk to be developed by ENISA under a publicly available database before the CRA applies. CECE also stresses the need for alignment with the Annex I.1(3) requirement to ensure legal certainty on manufacturers’ obligations: compliance with the Annex I.1(2) requirement should likewise be based on a risk assessment.

About CECE

CECE, the Committee for European Construction Equipment, represents the interests of 1,200 construction equipment manufacturers through national trade associations in Europe. CECE manufacturers generate €40 billion in yearly revenue, export a sizeable part of the production, employ around 300.000 people overall. They invest and innovate continuously to deliver equipment with highest productivity and lowest environmental impact. Efficiency, safety and high-precision technologies are key. See also www.cece.eu.