European Materials Handling Federation

European Commission proposal for a "Regulation on Horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)" (COM (2022) 454 final)

FEM position paper
03/03/2023

Executive Summary

The European Materials Handling Federation (FEM) welcomes the European Commission's proposal for a Cyber Resilience Act as a crucial step towards ensuring cybersecurity of products with digital elements in the European Single Market. However, FEM raises several concerns and suggests recommendations for EU policymakers to ensure that the proposed measures will strengthen cyber resilience without impeding European innovation and competitiveness.

The FEM concerns on the CRA proposal are as follows:

1. **Article 2 (Scope)**: the vague definition of "product with digital element" creates uncertainty for manufacturers and increases non-compliance risks. FEM suggests redefining the scope of the Cyber Resilience Act based on actual risk and providing clear guidelines to identify products that fall under it. In this context, FEM suggests alignment with the Radio Equipment Directive Delegated Act, defining the cyber risk of a product depending on its direct or indirect connection to a network.

2. **Article 11 (Reporting Obligations of Manufacturers)**: the timeframe is too short for manufacturers to notify ENISA about any actively exploited vulnerability and incidents having an impact in the security of their products with digital elements. It should be aligned with the revised Network Information and Security Directive (NIS 2). Moreover, the text of the Cyber Resilience Act, as per the European Commission proposal, does not specify how ENISA will use the information received.

3. **Article 57 (Entry into Force and Application)**: the 24-month implementation timeline proposed by the European Commission is insufficient for several reasons. It should be at least 48-month long to ensure that industry can comply with the regulation effectively.

4. **Annex I (Essential Cybersecurity Requirements)**: essential cybersecurity requirements should be rephrased in accordance with the New Legislative Framework. Clarity is also needed on how essential cybersecurity requirements apply to software as product (SaaP). Moreover, further clarification is needed on the requirement for a software bill of materials, such as the format in which it should be provided.

5. **Annex III (Critical products with digital elements)**: a more detailed list of critical products, with clear definitions, should be included in the legislation before its publication. Particularly, more clarity should be provided on what is meant by the term "secure elements". Moreover, in the case of a critical product assembled to a non-critical one, the conformity assessment of the critical product should be carried out only once by the manufacturer of the critical component itself, not by the manufacturer of the assembled product containing the critical component.

6. **Overlaps with other EU Legislation**: there are potential overlaps between the Cyber Resilience Act and other EU legislation, notably with the Radio Equipment Directive Delegated Act and the revised Network and Information Security Directive. Clarity and certainty in this matter should be provided to prevent unnecessary delays and costs in the application of the Regulation.

European Materials Handling Federation

Introduction

FEM, the European Materials Handling Federation, welcomes the European Commission proposal for a Cyber Resilience Act (CRA) as a crucial step towards ensuring the cybersecurity of products with digital elements in the EU.

With the digital transformation driving innovation in our industry, materials handling equipment have become smarter and smarter. This is notably the case for equipment with autonomous guide functions or including telematics devices which allow to send out and receive data. Sensors and other connecting devices make it possible to monitor equipment's activity and performance, and carry out some services remotely, such as maintenance and repair. These installations are often applied to equipment such as forklifts and mobile elevating platforms. Therefore, with our products increasingly relying on digital solutions, we believe that a coherent regulatory framework is necessary to further help manufacturers build the cyber resilience and security of their products, contrasting the rise of cyberattacks and hackings in the European Single Market.

While FEM supports the European Commission initiative for a CRA, the analysis of the proposal has given rise to several concerns which, if left unaddressed, could have a significant impact on our products. We understand that the proposed CRA intends to cover a considerably vast spectrum of products circulating in the European Single Market and because of this we would like to stress that the impact of such a Regulation on each covered sector must not be underestimated.

In this position paper, FEM outlines its concerns with the European Commission proposal for a CRA and provides recommendations for the EU policymakers to address these issues, to ensure that the proposed measures will strengthen cyber resilience without impeding European innovation and competitiveness.

1. **Article 2: scope**

The proposal does not clearly define what is considered as a "product with digital element", leaving room for interpretation. This vagueness can create uncertainty for manufacturers and increase the risk of non-compliance. Besides, as stated in the Radio Equipment Directive Delegated Act, a cyber risk for a product is not implied by the existence of digital elements, but by its direct or indirect connection to a network. It is consequently important for the EU to redefine the scope of the CRA based on the actual risk and provide clear guidelines to ensure that all products that fall under the CRA scope are clearly identified and subject to the appropriate cyber resilience requirements.

Additionally, FEM is pleased to see the inclusion of Recital 27, which clarifies that products with digital elements that fall under the default category and embed Annex III critical products will not be considered critical products themselves. While this is a crucial concept, FEM regrets that it is only mentioned in a recital – which is not legally binding - and not reinforced in the main body of the proposal through an article or equivalent. Therefore, FEM urges policy makers to incorporate relevant language into the main body of the proposal to ensure legal certainty.

Finally, we understand that the European Commission's intention is not to apply annex I section II requirements to products placed on the market before the date of application of the CRA. However, we would appreciate to see such statement in the binding part of the CRA.

2. **Article 11: reporting obligations of manufacturers**

FEM also raises concerns about the requirements stipulated in Art. 11 (1,2), stating that manufacturers must notify ENISA of any actively exploited vulnerability contained in the product with digital elements and of incidents having an impact on the security of the product with digital elements, within 24 hours of becoming aware of it. This time frame is too short. For this reason, FEM calls on policymakers to ensure alignment of reporting obligations of the CRA with the Revised Network and Information Security Directive, Directive (EU) 2022/2555. In the cited Directive, under Article 23.4, reporting to ENISA is to be carried out:

(a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

(b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise.

Therefore, FEM welcomes the obligation for manufacturers to issue an early warning to ENISA, within 24 hours of becoming aware of any active exploited vulnerability and incidents having an impact on the security of the product with digital network, followed by a notification containing further information, to be sent to ENISA within 72 hours of becoming aware of the relative active exploited vulnerability and incident.

Additionally, while FEM welcomes the EU efforts to attempt to track cyber vulnerabilities, the text does not specify how ENISA is supposed to put to use the information received.
FEM suggests that the EU clarifies these requirements to ensure that the industry understands what is expected of them.

3. Article 57: Entry into force and application

The 24-month implementation timeline proposed by the European Commission is insufficient for several reasons:

i. The standardisation request only allows 2 years for the development of harmonised standards, which is be very optimistic given the absence of existing harmonised standards for cybersecurity and the need to create new standards from scratch.
ii. Article 6(3) requires the European Standardisation Organization (ESO) to wait for the Delegated Act to further specify the product definitions in Annex III, but these Delegated Acts are only proposed to be adopted 12 months after the CRA's entry into force.
iii. The standardisation request cannot be submitted to the ESO until the CRA is published in the Official Journal of the European Union (OJEU).
iv. Manufacturers can only receive a presumption of conformity from harmonised standards after they are cited in the OJEU, which will likely occur several months after their publication by CEN-CENELEC.
v. The current lack of cybersecurity HAS consultants will most likely delay the assessment (and therefore the publication) of the many standards to be developed in order to cover the very broad scope of the CRA.
vi. The process of conformity assessment to the CRA is a new concept, and it remains unclear how much time will be required to accredit a sufficient number of Notified Bodies
vii. Manufacturers will need additional time to build an internal structure to comply with the new obligations.

Given these considerations, a transition period of at least 48 months is necessary.

4. Annex I: essential cybersecurity requirements

The requirement for products with digital elements to be delivered without any known exploitable vulnerabilities (Annex I, 1.2) applies to any part of the product at the delivery time and creates a high burden for manufacturers. Delivery is not a notion recognised by the New Legislative Framework (NLF). Therefore, FEM is asking for the replacement of the term "delivered" by "placed on the market".

Besides, the requirements attached to the notion "known exploitable vulnerabilities" can only be implemented provided a publicly available database listing those vulnerabilities is in place before the date of application of the CRA.

Additionally, clarity is needed on how this requirement applies to software as products (SaaS).

Finally, the vulnerability handling requirements and the requirement for a software bill of materials (SBOM) in Annex I of the CRA raise concerns the need for further clarification, such as on the format in which the SBOM must be provided.

5. Annex III: critical products with digital elements

We are also concerned about the critical class II products defined in the CRA under Annex III. Particularly, more clarity should be provided on what is meant with the term "secure elements" under the classification of class II products, on point 8. This term is very broad and not clearly defined, which could lead to different interpretations depending on the industry sector.

Secondly, while we understand that future Delegated Acts might provide a more extensive list of critical class II products, we suggest that a more detailed list of critical products, with clear definitions, should already be included in the CRA before its publication to avoid any ambiguity.

Thirdly, in the case of a critical product assembled to a non-critical one, the conformity assessment of the critical product should be carried out only once by the manufacturer of the critical component itself, not by the manufacturer of the assembled product containing the critical component. This will ensure that the burden of compliance is allocated to those who are best placed to address the cybersecurity risks.

6. Overlaps with other EU legislation

We agree with the provisions outlined in Article 7 and Article 9 of the CRA proposal, which stipulate that compliance with the CRA serves as an automatic demonstration of conformity with the cybersecurity requirements set forth in the General Product Safety Regulation and Machinery Regulation, respectively. However, we remain concerned about the legal ambiguity that may arise from potential overlap between the CRA and other legislation, such as the Delegated Act to the RED, Regulation (EU) 2022/30, and the Revised Network and Information Security Directive, Directive (EU) 2022/2555). We acknowledge the recognition of this issue by the Commission and strongly encourage the European institutions to provide clarity and certainty in this matter, to promptly prevent unnecessary delays and costs in the application of the Regulation.

European Materials Handling Federation

About FEM

FEM has represented European manufacturers of materials handling, lifting and storage equipment since it was founded in 1953. One of the largest mechanical engineering sectors, the European materials handling industry employs nearly 300,000 people and generates more than €60bn annual turnover.
More information: www.fem-eur.com