European Commission proposal for a Cyber Resilience Act

EGMF position paper

17 February 2023

EGMF – the European Garden Machinery Federation – welcomes the European Commission's proposal for a Cyber Resilience Act (CRA). We believe that this legislation is a necessary step towards ensuring the security and integrity of the digital infrastructure that is essential to the functioning of our economy and society.

We understand that the proposed Cyber Resilience Act intends to apply to products with digital elements, therefore covering a considerably vast spectrum of products circulating in the European Single Market. It is of foremost importance that its impact is not underestimated.

Today, as an immediate reflection of the digital transformation, an increasing number of outdoor power equipment can be connected to a network or a device. This is the case for all autonomous garden machines, such as robotic lawnmowers, and all machines which share data on their usage.

We believe that the proposed measures must take into account the characteristics of our industry and should strengthen their cyber resilience without undermining innovation and European competitiveness.

As the European federation representing the interests of major garden, landscaping, forestry and turf equipment manufacturers, we would like to highlight the specific concerns and challenges that our industry identified in the context of this legislation. These relate to overlaps with existing EU legislation, harmonised standards, essential product requirements and the transition period.

EGMF believes that the future Cyber Resilience Regulation should strengthen cyber resilience, while enhancing innovation that is an essential element for the European competitiveness.

To achieve this objective, EGMF recommends EU decision makers to:

- Avoid overlaps with already existing EU legislation
- Limit the development of harmonised standards to 'type-B' standards
- Amend the wording in Annex I to provide legal certainty
- Extend the transition period to at least 48 months

1. Overlaps with already existing EU legislation

EGMF supports that, in accordance with Article 7 and Article 9 of the European Commission proposal, compliance with the Cyber Resilience Act automatically provides for presumption of conformity with the cybersecurity requirements under the General Product Safety Regulation and Machinery Regulation respectively.
However, we remain concerned at the legal uncertainty that is caused due to potential overlaps between the Cyber Resilience Act and the Delegated Act to the Radio Equipment Directive (RED), Regulation (EU) 2022/30, Articles 3.3 d), e) and f). We note that the Commission recognises this potential regulatory overlap and EGMF therefore strongly encourages the EU policymakers to provide legal certainty in this matter for the benefit of all stakeholders.

A clear way forward must be identified as soon as possible in order to allow industry sufficient time to understand the actual requirements and the related compliance test.

Further, we very much welcome the text of Recital 27, which states that a product with digital elements that is categorised in the default category but which embeds an Annex III critical product will not itself be considered a critical product. This is a crucial concept, but EGMF regrets that it is only included in a recital and that there is no text in the main body of the proposal, i.e. an Article, that legally reinforces this concept. We therefore urge EU policymakers to include relevant text in the main body to provide legal certainty.

Moreover, we believe it is necessary to ensure that, in relation to the future Network and Information System Directive (NIS 2), no conflicting requirements are introduced.

2. Harmonised standards

EGMF welcomes the approach of the Cyber Resilience Act to make use of harmonised standards as the preferred way to describe a means to comply with the essential requirements.

We suggest strengthening this approach by initially limiting the development of harmonised standards to ‘type-B' standards (i.e. generic safety standards, dealing with one safety aspect or one type of safeguard that can be used across a wide range of machinery), rather than 'type-C' standards (i.e. machine safety standards, dealing with detailed safety requirements for a particular machine type or group of machines). This would reduce workload on the standardisation committees.

3. Essential product requirements – Annex I

Annex I.1.2 of the proposal states that: “*Products with digital elements shall be delivered without any known exploitable vulnerabilities*”. The word ‘vulnerabilities’ applies to any potential weakness in the security system, while ‘exploitable’ refers to any non-secured path which is known and can be used to access sensitive information.

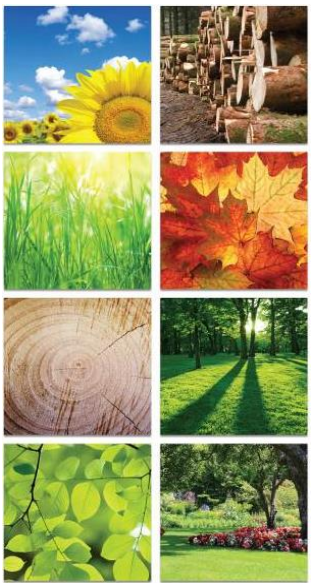
We believe that this wording is not precise enough to provide the legal certainty needed and must be reformulated in order to not risk disruption of supply chains. Therefore, EGMF suggests that this text is amended by deleting the word ‘exploitable’.

4. Transition period

EGMF believes that a 24-month application time proposed by the European Commission is not sufficient, for the reasons outlined below:

i) It is expected that the standardisation request will allow only 2 years for the development of harmonised standards. This seems rather optimistic given that there are currently no harmonised standards covering cybersecurity, meaning that entirely new standards will have to be developed.
ii) As per Article 6(3), the European Standardisation Organisation (ESO) would have to wait for the Delegated Act that will further specify the product definitions in Annex III, before working on the standards. However, these Delegated Acts are proposed to be adopted only 12 months after the entry into force.
iii) Moreover, the standardisation request cannot be sent to the European Standardisation Organisation before the publication of the Cyber Resilience Act in the Official Journal of the European Union (OJEU).
iv) Further, manufacturers will be able to obtain a presumption of conformity from harmonised standards only after they are cited in the OJEU. It is clear that this cannot happen on the same day that they are published by CEN-CENELEC and cannot therefore be cited in the OJEU until some weeks/months after their publication.
v) Finally, since conformity assessment to the Cyber Resilience Act is an entirely new concept, we wonder how much additional time the accreditation of a sufficient number Notified Bodies will take.

Because of all of these reasons, EGMF believes that a transition period of at least 48 months is required.



For further information, please contact: EGMF Secretariat, secretariat@egmf.org

The European Garden Machinery industry Federation – EGMF – has been the voice of the garden machinery industry in Europe since 1977. With 30 European corporate members and 7 national associations representing manufacturers for garden, landscaping, forestry and turf maintenance equipment, we are the most powerful network in this sector in Europe. Our members are responsible for employing 120,000 people in the EU, and in 2021 sold over 23 million units on the European Market.