Position Paper

Euralarm Position Paper on amendments proposed by the Council and ITRE committee of the European Parliament on EC proposal for a Cyber Resilience Act – 11 September 2023

1. Introduction

Euralarm, the European trade association representing the electronic fire safety and security industry, welcomes the results of the discussion within the Council and both ITRE and IMCO committees of the European Parliament. The utmost important amendments have been carefully assessed and recommendations supported by arguments issued by manufacturers and service providers from our sector are provided here.

The present position paper is intended for the 3 co-legislators and more specifically their representatives mandated for the trilogue.

2. Comments, recommendations and arguments on selected amendments

Article 2(1) on scope

The proposal from the Commission refers to the intended and foreseeable use while the amendment from ITRE extends to the capability of data connection. The experience with the RED DA on cybersecurity and privacy demonstrates how a scope based on the capability of the product is unclear and lacks legal certainty.

The initial proposal from the EC using the classical NLF wording "intended and reasonably foreseeable use" provides more clarity and should therefore be maintained in the final text.

In addition, the amendment proposed by IMCO and referring to external device or network is more proportionate to the risk and should be taken over.

We therefore suggest the following wording:

> "1. This Regulation applies to products with digital elements **placed on the market** whose **intended or reasonably foreseeable use** includes a direct or indirect logical or physical data connection to **an external** device or network."

Article 2(5) on exclusions from the scope

The Council proposal adds "public security" products in the exclusions to allow the Member States defining specific cybersecurity requirements for such products. Extending the scope of products for which national requirements are allowed is detrimental to the single market.

We support a European wide approach and therefore suggest to keep the original wording from the EC.

New Article 2(5b) from IMCO Committee on exclusions from the scope

This proposal writes:

> "*This Regulation **does not apply to the internal networks** of a product with digital elements if these networks have dedicated endpoints and are completely isolated and secured from external data connection.*"

We support the intent of this amendment as it renders the scope better proportionate to the risk. It would nevertheless gain in clarity by being rephrased as follows:

> "This Regulation **does not apply** to products with digital elements intended to be connected to **internal networks** if these networks have dedicated endpoints and are completely isolated and secured from external data connection."

New Article 2(4a) on exclusion of spare parts from the scope

Proposals from the Council and from ITRE are in line with the request that we expressed in our previous position paper. Such new article is warmly welcomed. However, the sentence limiting to "exclusively manufactured" is too restrictive as such spare parts could also be manufactured for e.g. selling out of the EU market.

The amendment proposed by IMCO fulfils the expectation and is therefore preferred:

> "This Regulation shall not apply to spare parts intended solely to replace defective parts of products with digital elements, in order to restore their functionality."

New Articles 4(1a) and 4(5) from the Council on free movement

These 2 amendments proposed by the Council do theoretically not prevent the free circulation of goods but could limit the possibility of use of these goods.

This is perceived as backdoors allowing for additional national requirements and we think therefore these articles should not be endorsed for the final text.

Articles 6(1), 6(2) and 6(3) and Annex III on critical products

Providing criteria in the legislation for classification of products implements the risk-based approach and brings clarity to the reasons why certain categories of products are listed in Annex III. It also allows for more concise subsequent paragraphs with the same result.

We therefore support the Council's approach for both 6(1) and 6(2).

In addition, part the amendment from ITRE solves the unclarity in case a critical product is embedded into a product from the default category and should be added to Council's proposal in 6(1):

> "The integration of a product of higher class of criticality does not change the level of criticality for the product it is integrated into."

Furthermore, Council's paragraph 6(2) should incorporate ITRE proposal for a stability period and should include a minimum transition period when categories are brought from a lower class to an upper class by stating:

> "The first such delegated act may be adopted at the earliest two years after entry into force of this Regulation and any subsequent delegated act may be adopted at the earliest two years thereafter. **In case these delegated acts intend to bring categories of products with digital elements from a lower class (i.e. default or Class I) to an upper class (i.e. Class I or Class II), they shall allow for a transition period of at least 36 months**".

Regarding paragraph 6(3), clarification on the definitions of categories of critical products should be available as soon as possible for the manufacturers of targeted products but also for the standardisers.

ITRE proposal for a maximum delay of 6 months after EiF should therefore be endorsed by the final text.

In consistency with the preference for Council's approach regarding Articles 6(1) and 6(2), the list of categories in Annex III as proposed by the Council should be chosen. In addition, any new category to be listed in Annex III shall match the criteria 6(1)(a) and/or (b).

New Article 10(2a) from the Council and ITRE on risk assessment

Both proposed amendments are not strictly necessary as risk assessment process is common to all NLF legislations. In addition, they can be too restrictive by finally requiring how the risk assessment should be achieved.

We therefore think none of these 2 amendments should be endorsed for the final text.

Amendments to Article 10(6) from the Council and ITRE on vulnerability handling

The product lifetime can depend on other aspects than its cyber resilience. The duration of the process for vulnerability handling should therefore be decoupled from the product lifetime. Also, the manufacturer should not be liable for vulnerabilities that are out of his control.

The proposal from ITRE properly introduces a "support period" and should be endorsed and complemented by the IMCO proposal as follows:

> "[…] and in accordance with the essential requirements set out in Section 2 of Annex I, **provided that it is within the manufacturer's control.**"

Amendments to Article 11 from the Council and ITRE on reporting obligations

The reporting delays in both 11(1) and 11(2) are very short and not sustainable, especially for SMEs, by requiring staff available across the weekends and bank holidays. The shortest reporting delays under RAPEX for safety issues are 3 days and the CRA should consider a similar approach.

The reporting process should therefore be set as a single step to be completed the working day after becoming aware of the actively exploited vulnerability/incident. This proposal aligns to the initial proposal from the European Commission for most of the days in a week and accommodates for the weekends and bank holidays.

Also, IMCO amendment to refrain vulnerability disclosure by ENISA until it is fixed and to notify on a "need-to-know-basis" is proportionate and should be endorsed:

> "Where a notified vulnerability has no corrective or mitigating measures available, ENISA shall ensure that information about the notified vulnerability is shared in line with strict security protocols and **on a need-to-know-basis**."

Regarding Article 11(4) on informing the users, we re-iterate our concern that, due to the supply chain between the manufacturer and the users, the manufacturer has not necessarily access to the users and therefore can't inform them. Furthermore, he can't identify who are the "impacted users" introduced by ITRE proposal.

We therefore support the amendment from the Council with some rephrasing to involve the whole supply chain between the manufacturer and the users.

Finally, the proposed reporting obligations have no time limitation. This means that the manufacturers shall keep in place and maintain **for ever** the means for the users to report vulnerabilities for each and every product. This is not sustainable. To ensure consistency with the requirement to handle the vulnerabilities during the support period, the reporting obligation should also be limited in time to the support period from the date the last individual product has been placed on the market.

Start paragraph 11(1) with:

"**Until the support period of the last individual product placed on the market has elapsed,** […]".

Amendments to Article 57 from the Council and ITRE on application

Standardisers need a decent time to prepare and adopt the numerous harmonised standards and the manufacturers need a decent time to adapt the products and processes and, finally, demonstrate their compliance with the essential requirements.

We therefore support a transition period of at least 36 months as proposed by ITRE and preferably 48 months. For the application of Article 11, 24 months as suggested by Council is a minimum and 36 months is preferable.

IMCO suggested the issuance of guidelines for non-tangible products. Such a guidance would be very helpful because coverage of non-tangible products in a NLF legislation is new.

This amendment should be endorsed by the final text:

"No later than 6 months after the date of entry into force of this Regulation, the Commission shall issue guidelines on how to apply the requirements in this Regulation to non-tangible products."

4. Conclusion

Euralarm appreciates the transparency efforts of both the Council and the Parliament by sharing their proposed amendments. They provide very interesting improvements to the original text from the European Commission.

We have commented some of these numerous amendments and provided arguments explaining the reasons why some amendments should be endorsed and others should not. We hope our arguments from the fire safety and electronic security perspective provide some added value for the trilogue.

We remain available to further discuss this position.

About Euralarm

Euralarm represents the fire safety and security industry, providing leadership and expertise for industry, market, policy makers and standards bodies. Our members make society safer and secure through systems and services for fire detection and extinguishing, intrusion detection, access control, video monitoring, alarm transmission and alarm receiving centres. Founded in 1970, Euralarm represents over 5000 companies within the fire safety and security industry valued at 67 billion Euros. Euralarm members are national associations and individual companies from across Europe.

Gubelstrasse 11 • CH-6300 Zug • Switzerland

E: secretariat@euralarm.org
W: www.euralarm.org

DISCLAIMER

Note: The English version of this document, GD-2023-016, is the approved Euralarm reference document.