# Position Paper

## Euralarm Position Paper on proposed Cyber resilience Act – 20 January 2023

## 1. A horizontal legislation on cybersecurity of products

Euralarm, the European trade association representing the electronic fire safety and security industry, has for more than 2 years asked for a horizontal legislation on cybersecurity for products instead of adding pieces of cybersecurity provisions in vertical legislations. The proposal for a Cyber Resilience Act pushed forward by the European Commission has therefore been carefully assessed by our members to highlight the principles that we find particularly beneficial to our industry, our customers and the users of our systems and the rooms for improvement.

This Position Paper provides our view on the elements of the proposed CRA that should be kept for the published legislation, identifies some unclarities that, if maintained, would lead our manufacturers into some legal uncertainty and proposes several amendments to the text.

## 2. Strengths of proposed CRA

The following principles implemented by the proposed CRA are appreciated as positive contributions to the European single market:

- the proposed legislation is based on the New Legislative Framework (NLF) and therefore benefits from decades of successful experience in product regulation;
- CE-marking will remain the mark for declaration of compliance, no additional logo specific to cybersecurity is enforced;
- the horizontality of the scope avoids a patchwork of various legislations addressing the same concerns;
- the intention to repeal delegated Regulation (EU) 2022/30 under the Radio Equipment Directive;
- the complementarity of the 3 sets of product, process and reporting requirements makes the proposal relevant to contribute to the reduction of the cyber risks;
- considering harmonised standards as the first choice for providing the technical details;
- leaving to the manufacturer the definition of the expected lifetime of the product;
- the link between the risk category and the compliance assessment procedure;
- the intention to allow for self-assessment for the large majority of products.

All these elements are in line with the answers we have provided during the public consultation on this initiative.

## 3. Identified concerns and proposals for improvement

Our assessment of the proposed Regulation and our discussions with the CRA team at DG CONNECT have identified some room for improvement in order to ensure legal certainty for the manufacturers and proportionality of the scope and the categorisation while maintaining the overall objective of increasing the cyber resilience of the European society.

Article 2(1) writes:

> *This Regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network.*

This wording of the scope assumes that any digital product capable to exchange data through a connection is susceptible to undergo or be part of a cyber-attack. This is not proportionate and the following example illustrates this. A smoke detector connected to a fire detection control panel via a bus connection is exchanging data reflecting the measured amount of smoke, detected fault and other status information. The bus is connecting many detectors and other fire detection components in a loop and so forms an isolated local network located inside the building and entirely managed by the control panel. The communication on the bus is commonly achieved by a proprietary protocol dedicated to this particular intended use. Such implementation makes any **cyber**-attack on the detector and on other field components on the loop practically impossible. Similarly, the detector and other field components on the loop cannot undergo any cyber-attack.

Another example is a conventional smoke sensor processing digital data inside the product and connected to another device to exchange purely analogue signals only (e.g. measured values). The manufacturer of such a product will have to undertake and maintain a conformity assessment procedure specific to the CRA even though the absence of any cyber risk is obvious. Malicious attacks (like cutting of a wire) are always possible on any interconnection but they are not necessarily **cyber**-attacks.

In order to render the scope better proportionate, we propose the following amendment:

> *This Regulation applies to products with digital elements whose intended or reasonably foreseeable use includes a direct or indirect logical or physical data connection to a device or network* ***and whose intended use and intended operational environment include the susceptibility to be cyber-attacked, to undergo a cyber-attack or to have personal data being compromised****.*

Article 2 defines the scope of the Regulation.

In the context of industrial product with long lifecycle and legacy like for security systems and fire safety systems, spare parts shouldn't be impacted by the Regulation in order to ensure the functioning, maintenance and reparability of long-lasting products.

We suggest excluding spare parts for products from the scope where the to-be-repaired product has been placed on the market before the application date of the CRA.

Articles 3(1) and 3(2) define "product with digital elements" and "remote data processing" as:

*'product with digital elements' means any software or hardware product and its remote data processing solutions, including software or hardware components to be placed on the market separately*

*'remote data processing' means any data processing at a distance for which the software is designed and developed by the manufacturer or under the responsibility of the manufacturer, and the absence of which would prevent the product with digital elements from performing one of its functions*

The first definition puts together two main elements: the product and its remote data processing. Although we understand from the discussions with DG CONNECT that the intention is to cover any digital product, this definition doesn't make clear whether each of these two elements taken separately has to be considered as fulfilling the definition of product with digital elements.

Example 1: a digital product without remote data processing under the responsibility of the product manufacturer, like a detector with a bus connection to a control panel from a different manufacturer. In this example, the product has no remote data processing as defined in Article 3(2). Therefore, it is unclear whether the detector alone is to be considered as a "product with digital elements" or not.

Example 2: a software (under the responsibility of manufacturer A) running in an alarm receiving centre receives data from many alarm systems (under the responsibility of manufacturers B, C, D etc.) In this example, it is unclear whether the software from manufacturer A alone is to be considered as a "product with digital elements" or not.

In order to clarify the definition of "product with digital element", we propose the following amendment:

*'product with digital elements' means any software or hardware product and its remote data processing solutions **(if any)**, including software or hardware components to be placed on the market separately*

Article 5(1) provides requirements for products by referring to Section 1 of Annex I. Item 1(2) refers to exploitable vulnerabilities.

An exploitable vulnerability does not necessarily lead to a risk to the product.

The requirement should be changed to "Products with digital elements shall be delivered without any known exploitable vulnerabilities **that would expose to unacceptable risk for the intended purpose**".

Article 5(2) provides requirements for processes put in place by manufacturers by referring to Section 2 of Annex I. Most of the items make reference to vulnerabilities and updates with the aim of providing updates free of charge and of disclosing the vulnerabilities.

Software vulnerabilities and software updates are targeted here but it is not explicitly stated. Enforcing hardware update could become very expensive.

Where the words "vulnerability" and "update" are used in text, they should be specified as "**software** vulnerability" and "**software** update".

The obligation to disseminate patches and make them available free of charge might not be fitting for the industry and B2B settings. In the industrial sector, while many patches are made available free of charge, the criticality and complexity of industrial systems and installations have led us to provide personalized services to clients to push the patching. While patching itself is free of charge, the personalized service to push and install the patch is commercialised under a contractual agreement.

A recital should be added to clarify that, for industrial products, the requirement to make the dissemination of the security updates free of charge does not cover the possible personalisation of the update which can be charged on a contractual basis.

Articles 10(6), 10(12) and 23(2) refer to the "expected product lifetime".

We understand by the corresponding provisions that this lifetime is defined by the manufacturer and we acknowledge this as a positive provision of the draft CRA in section 2 of this position paper. However, the document doesn't explicitly state that this lifetime can be defined by the manufacturer.

Where the wording "expected product lifetime" is used in text, it should be specified as "expected product lifetime **defined by the manufacturer**".

Article 10(10) provides requirements on information and instructions to the users and refers to Annex II for the content.

Item 2 of this Annex lists:

*"the point of contact where information about cybersecurity vulnerabilities of the product can be reported and received"*

It is unclear whether the "point of contact" needs to be put in place by the manufacturer or whether the European Commission will put such a common point of contact in place.

The text of the CRA should clarify who shall put in place the "point of contact".

Article 11(1) provides obligations of manufacturers to report actively exploited vulnerabilities to ENISA.

The reporting obligations have no time limitation. This means that the manufacturers have to 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 product lifetime or five years, the reporting obligation should also be limited in time to the product lifetime or five years (whichever is shorter) from the date the last individual product has been placed on the market.

Start paragraph 11(1) with "**From the placing on the market of the last individual product and for the expected product lifetime or for a period of five years after the placing on the market of a product with digital elements, whichever is shorter** [...]".

Article 11(4) about reporting obligations of manufacturers writes:

*"The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident."*

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.

Paragraph 11(4) should be rephrased to involve the whole supply chain between the manufacturer and the users.

Article 6(1) introduces categories of critical products by referring to the lists in Annex III. In addition, Article 6(3) empowers the European Commission to adopt delegated acts to make these lists of Class I and Class II critical products better defined.

Whether a product falls into the default category or is considered as a Class I or Class II critical product is of primary importance to know which compliance assessment procedure has to be applied. Nevertheless, no certainty on this categorisation will be gained soon. The current lists provided in Annex III are too vague to allow the manufacturers to assess the impact for their products. In addition, the delegated acts providing better detailed definitions will be available only 1 year before the applicability date of the CRA. Considering that it is unlikely to have harmonised standards cited in the Official Journal of the European Union (OJEU) at the applicability date, this leaves only 12 months to the manufacturers to have their products assessed by a notified body, should they be identified as critical products.

In order to grant a sufficiently long transition period to the manufacturers of critical products, to allow reasonable delay for the European Standardisation Organisation (ESOs) to prepare and adopt the harmonised standards and to give to the notified bodies the opportunity to get prepared and assess the critical products, the CRA should allow for at least 24 months after the adoption of the delegated acts referred to in Article 6(3) before the application of the CRA.

Annex III lists Class I and Class II critical products. From these lists, we stress the following items:

Class I, item 17: *"Firewalls, intrusion detection and/or prevention systems not covered by class II"*
Class II, item 4: *"Firewalls, intrusion detection and/or prevention systems intended for industrial use"*

Being the European trade association for alarm systems, we, as Euralarm, understand "intrusion detection systems" as electronic systems which intended use is to detect intruders breaking into a building and we understand "prevention systems" as possibly embedding fire prevention systems like fire detection and fire alarm systems and firefighting systems. From a discussion with DG CONNECT we have understood that "***cyber*** *intrusion detection and/or* ***cyber*** *prevention systems"* are targeted. This illustrates the need for clear definitions of these Class I and Class II categories of critical products, as expressed above.

The wording "intrusion detection and/or prevention systems" should be clarified by "cyber intrusion detection and/or cyber prevention systems"

Class I, item 22: *"Industrial Automation & Control Systems (IACS) not covered by class II, such as programmable logic controllers (PLC), distributed control systems (DCS), computerised numeric controllers for machine tools (CNC) and supervisory control and data acquisition systems (SCADA)"*

Class I, item 23: *"Industrial Internet of Things not covered by class II"*

Referring to these items about IACS and IoT, we can't conclude whether Fire Detection and Fire Alarm systems, Fixed Firefighting systems, Intruder and Hold-up Alarm systems, Video Surveillance systems, Access Control systems etc. which are intended for installation in industrial environments are to be considered industrial IACS or industrial IoT systems and thus Class I or Class II products. This further illustrates the need for clear definitions of these Class I and Class II categories of critical products, as expressed above.

Furthermore, we strongly believe that considering any industrial IACS or industrial IoT device as Class I critical products is going beyond a proportionate approach. Many of such products and systems, even if intended for industrial do not necessarily expose to critical cyber risks.

The need for clear definitions of critical product categories long before the applicability date of the CRA is repeated here. In addition, the consideration of industrial IACS and IoT devices as Class I or Class II should be refined to make these categories better proportionate to the actual risks.

Annex III lists several hardware and software components like microprocessors, microcontrollers, privileged access managers, password managers, network management systems, application configuration management systems, remote access/sharing software etc.

We understand that these are the components referred to in the definition for "product with digital elements". However, it is unclear in the CRA provisions whether (i) these components shall be considered as Class I or Class II critical products only when they are placed on the market as separate components or whether (ii) any product embedding such components shall also be considered as critical products of the same class. Having noted that the intention of the European Commission is to have 90% of the digital products falling into the default category, we understand that option (i) above is the actual intention and Recital (27) is supporting this understanding. Nevertheless, the legal provisions of the CRA don't state it clearly.

The legal provision of the CRA should clarify that components referred to in Annex III are categorised as such when they are placed on the market separately.

Article 8 tries to explain the articulation between the proposed CRA and the cybersecurity provisions of the proposed Regulation on Artificial Intelligence.

The high complexity of this Article illustrates the increasing complexity observed in general in the recent proposals from the European Commission like sustainability provisions in the proposed revised Construction Products Regulation (CPR) in addition to the proposed generic Regulation on Ecodesign requirements for Sustainable Products (ESPR) or a proposed Liability Directive for Artificial Intelligence (AILD) in addition to the proposed revised Product Liability Directive (PLD). This increasing complexity is against any simplification of the legislation, decreases the legal certainty for the manufacturers and ultimately puts the single market at risk.

Our analysis of this Article 8 led us to summarise it with the following table:

<table>
<tr><td></td><td></td><td colspan="3">CRA classification</td></tr>
<tr><td rowspan="4">AI Act classification</td><td></td><td>Non-critical</td><td>Critical<br>With application hEN cited in OJEU</td><td>Critical<br>With mandatory third-party assessment</td></tr>
<tr><td>Non-high-risk AI system</td><td colspan="3">Requirements and conformity assessment procedures from both acts apply separately</td></tr>
<tr><td>High-risk AI system<br>Self-assessment allowed</td><td colspan="3" rowspan="2">Products complying with CRA requirements are deemed to comply with AI Act cybersecurity requirements<br>CRA conformity assessment procedure shall apply for CS requirements<br>AI Act conformity assessment procedure shall apply</td></tr>
<tr><td>High-risk AI system<br>With mandatory third-party assessment</td></tr>
</table>

Assuming this analysis is correct, we have identified that by not having considered non-high-risk AI systems in Article 8 deprives them from a privilege granted to high-risk AI systems: products complying with CRA requirements are deemed to comply with AI Act cybersecurity requirements.

Article 8 should state that non-high-risk AI systems complying with the CRA requirements are deemed to comply with the AI Act cybersecurity requirements.

Article 57 sets the application date of the reporting obligations and of the whole Regulation at 12 months and 24 months, respectively, after the entry into force of the Regulation.

Considering the extremely wide scope of the CRA (far wider than the one of the Delegated Regulation under the Radio Equipment Directive), the time needed to redesign the full products portfolio and to assess their compliance with the new requirements and the numerous standards to be developed to cover that wide scope of products and the processes to be implemented by the manufacturers, the 24 months delay seems unreasonable.

Article 57 should set the application date of the CRA 36 months after the adoption of the delegated acts referred to in Article 6(3).

Setting the application date of Article 11 on reporting obligations at 12 months after the date of entry into force is unreasonable given that if some of the products will not be ready by that time, the reporting will be incomplete.

Article 57 should align the application date of Article 11 with one for the whole CRA.

The standardisation request cannot be offered to the ESOs before the publication of the CRA in the OJEU.

Euralarm is closely involved in the current standardisation process for the development of the harmonised standards supporting the Delegated Regulation under the RED. The very tight deadline puts a lot of pressure on the standardisers and on CEN-CENELEC. Such a pressure implies the requisition of a lot of resources. This level of pressure should be avoided when the same process starts in support of the CRA. On one hand, we understand that part of the work done under the RED will be reused to the benefit of the CRA and we acknowledge that, globally, 90% of the products can be assessed under Module A (self-assessment) without harmonised standards cited in OJEU. On the other hand, we envisage the large number of standards to be produced in order to cover all the product categories listed in Annex III and to cover the essential requirements on processes to be implemented by the manufacturers.

The ESOs and the stakeholders should be involved as early as possible in the preparation of the standardisation request to be offered at the time of entry into force of the CRA. In addition, the need for a 36 months transition period already expressed above is repeated here.

## 3. Conclusions

Euralarm highlights the positive principles found in the proposed CRA and requests the co-legislators to keep them for the final version of the Regulation.

We have highlighted the room for improvement by providing argued concerns and put forward proposals to clarify the text and render the Regulation better proportionate. We invite the co-legislators to carefully consider them.

We remain available to further discuss these proposals.

## 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-2023-001, is the approved Euralarm reference document.*