European Semiconductor Industry Association

# POSITION PAPER

## CRA implementation in the semiconductor industry

*Brussels, 15 September 2023*


## Executive Summary

On 15 September 2022, the European Commission published its proposal for a regulation on horizontal cybersecurity requirements for products with digital elements, the ***"Cyber-resilience Act"*** (**CRA**). The European Semiconductor Industry Association (ESIA) welcomes the CRA and its goal to integrate cybersecurity requirements into the internal market framework in line with the EU legislation for product safety. The semiconductor industry is present in virtually every application. From ground and air transportation to passports, payment cards, terminals, servers in data centres, desktop computers, sensors, etc., fulfilling a crucial element in the whole domain of the CRA legislation.

In view of the upcoming trilogue, ESIA would like to draw the attention of the policymakers to the following policy priorities that would help improve the CRA text:

- The one-size-fits-all approach of the regulation adds complexity for different product types, with different commercial, technical, and operational functions.
- The act should come with a realistic transition period of at least 48 months to allow companies to move toward adoption. This should also be the case for any subsequent updates, including but not limited to Delegated and Implementing Acts.
- The conformity assessment mechanisms should consider the existence of industry common practice standards and certification to achieve the ambitious goals of the regulation.

Implement the expert group, with thematic sub-groups, to address key elements of the regulation with industry collaboration.



Rue de la Duchesse 11/13
1150 Brussels
Belgium

Tel.: +32 2 290 36 60
Fax: +32 2 290 36 65
secretariat@eusemiconductors.eu
www.eusemiconductors.eu



ESIA is an industry association under the umbrella of
EECA: European Electronic Component Manufacturers' Association
EU Transparency Registry: 22092908193-23

# I. Product Diversity

EISA believes in distinguishing between components and finished products. There is a risk of adding unnecessary complexity by using the one-size-fits-all approach for security concerns derived from the nature of different technologies:

- hardware at the component level,
- software-only products as components,
- product platforms made of hardware and software components,
- hardware as the end-devices, and
- software-only products as applications or as-a-service.

Across those product categories, products will have different risk levels, and security conformance concerns ranging from the method to demonstrate conformance with the essential cybersecurity requirements, vulnerability management, product maintenance, etc.

Security dependencies are overlooked in the CRA proposal. Some end-devices will rely on the security services provided by platforms or components. This might have potential implications for the conformity assessment and vulnerability management of their products.

The hardware at the component level (semiconductors) and end-devices are far away from each other from a supply-chain perspective. For general-purpose components going into distribution channels, requirements like those from the regulation in the context of vulnerability management, notifying customers of potential vulnerabilities result in an almost unsolvable conundrum for the whole supply chain answering the question: who's the "*customer*"?

Unlike the majority of new legislative framework (NLF) legislations, the CRA does not distinguish between components and finished products. This means that potentially every single chip will have to be CE-marked, as it is considered a product. Some aspects of the CRA could be difficult to implement for certain technologies e.g., semiconductors.

**ESIA strongly recommends that products and their components should not be brought all to the same level, in terms of cybersecurity / resilience provisions:**

- **Clear definition of product types and classes**
    - Clear product definitions are very important, providing legal certainty and helping manufacturers prepare for the CRA implementation. Having a clear taxonomy is critical for products that, according to its definition, might end up in one class or another.
    - Within the semiconductor industry, this is particularly relevant as new technologies evolve and lines are crossed. For example: What category should a neural processing unit (NPU) need to be placed in? What qualifies as hardware security modules (HSMs)?
    - In this context, the concept of "*partially completed product with digital elements*", introduced in the Committee on the Internal Market & Consumer

Protection (IMCO) opinion of the European Parliament, should be considered an interesting way to solve the issue raised by the too broad definition of products with digital elements.

  - ESIA supports the proposal of the Council to adapt Annex III, especially classes I and II, in order to ensure that components such as general-purpose microprocessors are classified as non-critical.

- **Manufacturers guidance**

  - Additional guidance for non-general purposes integrated circuits (ICs) is needed, especially those dedicated to health and ground transportation markets, both exempted from this regulation. For example, in the automotive sector, the lack of guidance would result in additional burden and costs for semiconductor suppliers because original equipment components and systems (and their respective original replacements) are already subject to the automotive regulation requirements[1].

  - Guidance is required on how to qualify specialised products as some of them might need to be qualified for compliance within the specialised markets as well.

# II. Vulnerability Management

- While reporting obligations are necessary to ensure that consumers can benefit from products with digital elements that are secure, the current Article 11 creates more security risks. Manufacturers aware of maliciously exploited vulnerabilities should focus on mitigating them, which requires confidentiality and time. In any case, there should not be a reporting of any vulnerability without a mitigation in place first.

- The use of the term "*known*" in the context of the "*known exploitable vulnerabilities*" definition[2,3] is not clear. Secret services, government authorities, and public databases are all sources of knowledge. Ambiguity can drive unnecessary efforts adding cost and complexity.

---

[1] Recital (13); EUROPEAN COMMISSION (15/09/2022). *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Text with EEA relevance), COM(2022) 454 final*, p. 16-17, EUR-Lex. URL: https://eur-lex.europa.eu/resource.html?uri=cellar:864f472b-34e9-11ed-9c68-01aa75ed71a1.0001.02/DOC_1&format=PDF (retrieved 15/09/2023)

[2] Article 11(1a)(b); Annex I(1)(3)(aa); General Secretariat of the Council (31/08/2023). *Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/102 - Mandate for negotiations with the European Parliament, ST 12536 2023 INIT*, p. 79 &136, Council of the European Union. URL: https://data.consilium.europa.eu/doc/document/ST-12536-2023-INIT/en/pdf (retrieved 15/09/2023)

[3] Annex I, Part 1(3)(-a); European Parliament 2019-2024 (26/07/2023). ****I DRAFT REPORT on the proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (COM(2022)0454 – C9-0308/2022 – 2022/0272(COD)). Rapporteur: Nicola Danti, PE745.538v02-00*, p. 219-220, Committee on Industry, Research and Energy. URL: https://www.europarl.europa.eu/doceo/document/A-9-2023-0253_EN.pdf (retrieved 15/09/2023)

- The industry takes notice of different processes for addressing vulnerabilities. There is a difference between patching and mitigating vulnerabilities across the different risk-model-driven applications: from products with a few updates and used on highly secure applications, to those with continuous product updates on applications with basic security concerns. ESIA recommends following a risk-based model for managing vulnerabilities, as it is used for product classifications and conformance methods, reflecting the realities of the technology and supply chain for the different product requirements[4].
- In certain cases, the best approach will be to wait longer than 72 hours for reporting as manufacturers address the root cause and find mitigation, or eventually a solution to a particular vulnerability[5,6]. This is particularly relevant for general-purpose semiconductors having multiple and different contexts of use.
- It must be considered that addressing vulnerabilities in semiconductors is far from trivial, and fixing hardware issues is much more complex than deploying new software.

## III. Implementation of the Regulation

There are still a few unanswered questions within the regulation that will be addressed after the implementation, via Delegated or Implementing Acts. Definitions like software bill of materials (SBOM), use of security certification schemes from CSA for conformance, applicability, and scope of other conformance mechanisms, are some of the examples of key pieces of information that manufacturers require to prepare for a successful CRA implementation.

**ESIA strongly recommends that each of those Acts incorporates its own transition time, rather than applying for each of them the original implementation from the CRA to Delegated and Implementing Acts introduced during the transition period.**

## IV. Conformance Mechanisms

Developing standards takes time, it is a complex exercise, and on top of it, there is only a very small number of individuals, experts in the domain, who actively contribute to this activity. As a result, developing one single standard takes no less than a year in a best-case scenario. This applies to public-private and industry-driven standardisation organisations. The development of harmonised standards (hENs) for the "*Radio Equipment Directive*" (RED) and schemes for the CSA are some examples of the amount of effort, and time, that is required to launch one standard.

Developing a series of hENs for the large number of product types described in the regulation represents a challenge of a magnitude hardly seen before in the standardisation world, while there are no new resources added to the existing, already stretched pool of experts.

[4] Article 10(3); EUROPEAN COMMISSION (15/09/2022). *Op. cit.*, p. 38-39.
[5] Article 11(1a)(a); Article 11(1a)(b); General Secretariat of the Council (31/08/2023). *Op. cit.*, p. 79.
[6] Article 11(1a); European Parliament 2019-2024 (26/07/2023), *Op. cit.*, p. 64-65.

**To provide the industry with sufficient, mature conformance mechanisms, ESIA recommends the following points.**

- **Use existing public and private standards and schemes to show conformance**
    - There are existing security standards and schemes, pursuing similar goals to those in the "*Cybersecurity Act"* (CSA), including at international level as proposed by the Parliament (Recitals (32), (38), (41) and Article 18(1)).
    - With the proper mapping, supported by expert groups, and activated by applicable acts to different product types, it brings best practices in support of the CRA implementation.
    - Efforts should also be put into how standards and certifications work together to ensure easy adoption for end-product manufacturers.
    - This requires that common specifications are taken to a same level of conformance as any other mechanisms, away from the "*last resource*" as portrayed by the current text in the regulation.

- **Effective use of CSA security schemes for CRA conformance**
    - This requires a clear definition of CSA assurance level requirements, its equivalence, and applicability for the different product types and classes, as defined by the CSA regulation according to basic, substantial, and high.
    - The CSA security schemes for CRA conformance should not be based on hENs. From timelines, objectives, etc., they are different, parallel mechanisms of conformance that should not be mixed to prevent unnecessary complexity.
    - Priority needs to be given to mechanisms addressing the presumption of conformity for the manufacturers using CSA schemes, as currently proposed by Parliament (Article 18(4)).
    - The publication of the Rolling Work Program for the European Union Agency for Cybersecurity (ENISA) to develop certifications is very much necessary at this stage for companies to plan how to comply with the CRA requirements.

# V. Expert Group

The CRA addresses software and hardware using the same parameters. There are key differences between the two product categories:

- The software cannot be executed without hardware, while hardware can perform tasks without software.
- Software, if not tangible, cannot be touched, while the hardware is tangible.

- Software is debugged in case of a problem and reinstalled if the problem is not solved. Hardware, on the other hand, might need to be replaced if mitigation countermeasures to the problem are not found.

The semiconductor industry, being largely a hardware industry supported by software, acknowledges those differences and calls for an expert group[7] working on this domain for the implementation of the CRA. We believe a dedicated group will always work better by addressing specific nuances of each sector[8]. Once the regulation is in place, this group could oversee the development of product-specific provisions including taxonomy, product classes, vulnerability management, cross-regulatory compliance (for example the "*trusted chips*" initiative from the "*EU Chips Act*"), etc. Such product-specific provisions could be covered in Delegated Acts. It is important that the members of the expert groups are chosen based on criteria of competency and expertise.

ESIA supports the idea of creating a semiconductors expert group, with a broad and open industry participation, where the CRA spirit can be translated, and implemented via Delegated Acts. The semiconductor industry supports executing effective, scalable, and commercially viable ways to reach the CRA objectives of building a cyber resilience market.

This expert group could greatly contribute to the implementation of the CRA for the semiconductor industry by addressing product classes, taxonomy, conformance mechanisms, and vulnerability management mechanisms.

**ESIA is ready and willing to collaborate on this effort, contributing to the expert group addressing key elements of the regulation applicable to the semiconductor industry for a successful CRA implementation.**

[7] Article 6a; European Parliament 2019-2024 (26/07/2023), *Op. cit.*, p. 54-56.
[8] Article 18(5); General Secretariat of the Council (31/08/2023). *Op. cit.*, p. 92.

**For further information:**

Hendrik Abma
Director-General
European Semiconductor Industry Association (ESIA)
Tel: + 32 2 290 36 60 • Web: https://www.eusemiconductors.eu/

***ABOUT ESIA***

*The European Semiconductor Industry Association (ESIA) is the voice of the semiconductor industry in Europe. Its mission is to represent and promote the common interests of the Europe-based semiconductor industry towards the European institutions and stakeholders in order to ensure a sustainable business environment and foster its global competitiveness. As a provider of key enabling technologies, the industry creates innovative solutions for industrial development, contributing to economic growth and responding to major societal challenges. Being ranked as the most R&D-intensive sector by the European Commission, the European semiconductor ecosystem supports approx. 200.000 jobs directly and up to 1.000.000 induced jobs in systems, applications and services in Europe. Overall, micro- and nano-electronics enable the generation of at least 10% of GDP in Europe and the world.*