EUROPEAN CYBER SECURITY ORGANISATION

POSITION PAPER

Cyber Resilience Act

ECSO Working Group 1 and Policy Task Force

Created: December 2022
Updated: June 2023

ECSO Position Paper on the Cyber Resilience Act

Executive summary

The **European Cyber Security Organisation (ECSO),** representing the backbone of the European cybersecurity ecosystem, welcomes the ambitious proposal for a Cyber Resilience Act (CRA). In this peculiar moment when the European Union is facing significant strategic cyberattacks by state and non-state actors threatening public and private systems, ECSO's Members are proud to contribute to the digital security of EU citizens, companies, and infrastructures. ECSO supports the work done over the years by the European Union to secure the European Digital Single Market with legislations and investments, and continues to advocate for more **European Strategic Autonomy** and **Cyber Resilience**.

ECSO has consulted with its diverse members' base on the CRA and came forward with the following position paper. ECSO Members welcome the proposal of the CRA and support its objective; at the same time, they provide suggestions to the co-legislators to ensure that its implementation would not impose unnecessary burden to the European industry while keeping all its benefits for the users of products with digital elements.

ECSO asks **guidance** to the European Union on **how companies should comply with this regulation**, especially when there is an interplay with other legislations like the Cybersecurity Act, NIS2 Directive, DORA, AI Act, and others. ECSO believes that a thorough mapping of global existing criteria and standards for conformity assessment should be done for the benefit of both the users, the producers, and the third-party certifiers.

The European cybersecurity ecosystem needs to have a proper understanding of how products will be categorised, knowing in advance whether their products will fall under the default category, Class I or Class II. For this reason, it is essential for companies to have a clear **methodology for risk assessment and product categorisation** so that they can adjust their internal processes and invest for the right conformity assessment methods.

ECSO supports European **small and medium enterprises** and asks the co-legislators to consider how CRA will affect SMEs to ensure that the implementation will be manageable for all. The CRA will strengthen the security of the whole supply chain; for this reason, manufacturers of products with digital elements will save money as they will purchase more secure products from suppliers that will also be CRA-compliant. At the same time, the CRA will require investments from companies to comply with its obligations. As every company is unique, it is impossible to predict exactly the impact of this cost redistribution. To minimise its impact on SMEs, ECSO recommends **aligning the CRA with existing EU legislation** – like the Cybersecurity Act, NIS2 Directive, DORA, AI act – whenever possible and **provide guidelines** and **financial support to** help SMEs to better comply with the CRA.

Regarding the *timing* of reporting obligations, to minimise the burden on companies, the CRA should be **aligned with the NIS2** Directive and establish a **24-hour** deadline for **early warning** and **72-hour** deadline for **notification.** To ensure transparency, convenience and impartiality,

the **reporting should be done to ENISA**. The interplay between the CRA and other legislations should also be clarified, promoting harmonisation wherever possible.

CHAPTER I – General provisions (Art. 1-9)

On **Art. 2** ECSO supports a **broad scope** of the CRA for both hardware and software and believes that products like endpoint Software as a Service solutions should also be included in the scope. This is because of the increased use of cloud in the digital transformation and the fact that more products are being designed, created, and operated in a cloud environment.

Regarding the interplay with other legislations, ECSO asks the co-legislators to **clarify the overlaps with all other more vertical and sector-specific legislations** in order to facilitate compliance. Therefore, the link with the Network Code on Cyber Security (NCCS) for the electricity sector, the European Health Data Space regulation, the NIS2 directive, the Cybersecurity Act, the delegated Act on the Radio Equipment Directive, and DORA package should be made clear. The European Commission should provide **guidelines** to companies to understand what **requirements** they have to comply with and to whom they have to **report**.

With reference to **Art.3** on definitions, ECSO advocates for the following adjustments:

- Art.3(15) "*endpoint*" → cloud-deployed assets like apps, websites, etc., need to be included not only devices. Regulation (EU) 2019/1020 refers to "online interfaces".
- Art.3(37) "*software bill of materials*" → harmonised standards for software bill of materials are needed to make it readable, comparable, and transferable in both human and machine-readable format.

Regarding **Art. 4(2)** on **free movement**, ECSO supports the amendment suggested by MEP Ignazio Corrao: "*Member States shall not prevent the presentation and use of a prototype product with digital elements which does not comply with this Regulation, provided that the availability is limited in time and geographical area and is supplied exclusively for testing".*

With reference to **Art.5 *Requirements*** *for products with digital elements,* ECSO considers that Art.5(1) is formulated in a way that adds unneeded confusion to the legal text. It would be sufficient for the Regulation to state: "*Products with digital elements shall only be made* ***available on the market where they meet the essential requirements*** *set of in Section 1 of Annex I*".

To better fit the market reality, a product with digital element should be **compliant** with the CRA at the **moment it is sold on the market and when it receives security updates** from the throughout its life cycle. The user should be allowed to freely customise the product according to their needs, and the producer should not be held liable for any security incident following customisations outside the contractual agreement.

Regarding **Art.6**. ECSO believes that when the European Commission determines the cybersecurity risk linked with a product, it **shall consider at least two of the following criteria, namely criteria a) and one of the others.**

(a) the cybersecurity-related functionality of the product with digital elements and whether the product with digital elements has at least one of following attributes:

(i) it is designed to run with elevated privilege or manage privileges;

(ii)it has direct or privileged access to networking or computing resources;

(iii) it is designed to control access to data;

(iv) it performs a function critical to trust, in particular security functions such as network control, endpoint security, and network protection.

(b) the intended use in a critical function in critical industrial or by essential entities of the type referred to in the Annex [Annex I] to the Directive (EU) 2022/2555 (NIS2);

c) the intended use of performing critical functions or for processing of personal data;

d) the potential extent of an adverse impact, in particular in terms of its intensity and its ability to affect a plurality of persons;

e) the extent to which the use of products with digital elements has already caused material or non-material loss or disruption or has given rise to significant concerns in relation to the materialisation of an adverse impact.

CHAPTER II – Obligations of economic operators (Art. 10-17)

In **Art. 10(1)** and **Art 10(4)**, it is important to state to what extent the manufacturer is responsible for the **supply chains** of its products. The text should specify the level of due diligence required and the responsibility that can be transferred to suppliers.

Art. 10 (5) refers to the need to **update the risk assessment** of the product by keeping into account new vulnerabilities and security incidents. A clarification is needed to understand whether the update should be internal, or whether the manufacturer shall provide the update to third parties.

Regarding **Art. 10(6)**, about the product life cycle, ECSO supports the amendments proposed by MEP Nicola Danti to let manufacturers decide about the length of the product life cycle and allow third parties to issue security updates on behalf of the manufacturer if the life cycle of the product is less than 5 years.

Regarding the timing of reporting obligations, to minimise the burden on companies, the CRA should be **aligned with the NIS2** Directive and establish a **24-hour** deadline for **early warning** and **72-hour** deadline for **notification.** To ensure transparency, convenience and impartiality, the reporting should be done to ENISA. Finally, for every report and notification that a manufacturer sends to ENISA, a response shall be given without undue delay to inform the manufacturer that its report has been well received and to follow up on the next steps.

ECSO would also like to highlight the fact that entities belonging to the **financial sector** are already falling under the scope of DORA and NIS2 and would risk undergoing multiple reporting obligations for security incidents, having to report to ENISA (CRA), the national authorities (NIS2), and the financial supervisors (DORA). A similar situation exists also for the **energy sector** that falls both under the scope of the NIS2 directive and the Network Code on Cyber Security. These situations should be clarified with **dedicated guidelines and harmonisation** promoted whenever possible.

The current text obliges producers to make available and disseminate patching free of charge. In the **industrial sector**, while patching is usually made available free of charge, the criticality and complexity of industrial systems and installations have created a situation for which personalised services to clients to push the patching are sold separately. It follows that, the mandatory patching **should be free of charge at least for the last version of the product or service. The personalised service to push and install the patch in an industrial environment**

could be commercialised under contractual agreement if the user needs assistance or external support in pushing the patches. Other similar business models – where the paid support to old versions supports the development of new ones – should be safeguarded. ECSO therefore encourages the co-legislators to clarify the text on **the definition of "disseminated"** (Annex I point 2.(8)), restricting it to the **provision of the patch** and not to its installation on the product, which is subject to the specifications of the industrial process and user choices.

CHAPTER III – Conformity of the product with digital elements (Art. 18-24)

Regarding the interplay with existing industry standards on cybersecurity, a thorough **mapping of all existing global standards** is required to better identify those that could be applied to the CRA. The European Commission should map existing standards and update the list of applicable ones regularly. Furthermore, the European Commission should create additional cybersecurity certification schemes under the EU Cybersecurity Act to facilitate compliance with the CRA.

We would therefore encourage the European institutions to take the long-term industry cyber security investment into account and to value it by creating a **compatibility mechanism**. This compatibility mechanism should rely on already adopted European industrial security standards framework (**EN IEC 62443**) including associated available IACS certification schemes operated by accredited European Conformity Assessment Bodies (CAB) actors.

In addition, the referred cybersecurity ecosystem allows European industry to have an **international reach and market recognition inside and outside Europe** for their products with digital elements.

ANNEXES OF THE CRA– Annexes I-VI

Annex I Essential Cybersecurity Requirements

To date, Annex I point 1.2 of the CRA reads: "***Products with digital elements shall be delivered without any known exploitable vulnerabilities***". ECSO invites the co-legislators to clarify the definition of known exploitable vulnerabilities by saying that these would be the ones contained in **the EU vulnerability database to be set up by ENISA**, in accordance with the NIS2 Directive. Furthermore, ECSO stresses the importance of mentioning the notion of "**vulnerability handling" in the main text of the Regulation** and not only in Annex I.2.

Annex III | Critical products with digital elements

Regarding Annex III, ECSO believes that Class I and Class II should remain as a **comprehensive list of critical products** as it was in the original proposal of the Commission and as MEP Nicola Danti (ITRE) proposed to keep. Users of critical products require higher assurance of these products.

Annex VI Conformity assessments

It is important that a company's confidential information does not become public without consent during the conformity assessment procedure. For this reason, under EU-type examination, based on Module B point 5, additional text should be added to state that **confidential information or trade secrets** of the manufacturer shall be kept confidential and used only by the third-party certifiers to assess the compliance.

Finally, in relation to conformity based on full quality assurance under Module H section 3.3 and 4.3, ECSO highlights that further details shall be envisaged in order to emphasise that any confidential information or **trade secrets of the manufacturer shall be kept confidential**.

Other recommendations

ECSO strongly supports the idea that all the IoT vendors – not only software but also hardware manufacturers – should adopt an efficient **DevSecOps** approach and a **Vulnerability Disclosure Policy (VDP)** as horizontal cybersecurity requirement for all digital products and ancillary services that are placed on the European market. The above-mentioned procedure should cover the **whole life cycle of the product**. Adopting a vulnerability disclosure policy facilitates the emergence of collective cybersecurity responsibility which will increase the trust in the digital market. The European Union through the CRA should propose a harmonised approach for the use of VDP and incentivise supply-side actors in treating vulnerabilities more effectively. ECSO would welcome **economic and legal incentives** to the use of VDP solutions implementing global standards as the ISO/IEC 29147 ("Vulnerability Disclosure") and ISO/IEC 30111 ("Vulnerability Handling") standards.

Contact person

For any questions or comment feel free to contact:

Francesco BORDONE – Manager for Cybersecurity Policies

Email francesco.bordone@ecs-org.eu T: +32 492 11 36 72