10 May 2023, Brussels

Joint Industry Statement on the Cyber Resilience Act

The proposed Cyber Resilience Act (CRA) will for the first time build a horizontal framework for cybersecurity requirements across products with digital elements.

We welcome the work of the European Parliament's ITRE and IMCO rapporteurs on many aspects of the proposal. With a new approach to regulating cybersecurity, we strongly support the development of guidelines and the related creation of an Expert Group involving industry, which will be essential in providing all players with the necessary tools to understand how to apply and adapt the new rules.

More broadly, however, we believe additional changes are needed to ensure that the CRA's ambition can be met. The CRA's obligations must be clear, actionable, and reflect market dynamics.

We encourage the European Parliament and the Council to consider the following aspects:

1. An extended **implementation period**:
    - Overall, to the benefit of industry and competent authorities alike in ensuring the right standards and resources are in place for compliance;
    - To avoid disproportionate burden for manufacturers that have to redesign their complete hard- and software architecture.
2. Further clarifications on the broad scope. More in particular, the CRA's inclusion of **software as a product** requires further clarification of certain notions in order to avoid overlaps and an even broader scope:
    - **Open source software**, if not monetized in a final product which has been 'placed on the market', must be excluded by narrowing the wide concept of commercial activity.
    - **Software as a service** already covered by NIS2 should be clearly specified to not fall into the CRA's scope by avoiding uncertain references to **remote data processing**.

- All **spare parts are to be excluded**, as they are already covered by the compliance of the products with digital elements they are to replace or be integrated in.

3. Consistent with other product legislation,[1] the CRA must acknowledge the **partially completed nature of components**. Components cannot be assessed independently from the other products they are intended to be incorporated into. Considering all components finished products by default will result into undue burden and uncertainty for all manufacturers, and ultimately higher prices for consumers. As such, a potential situation arises that components will have to undergo conformity assessment twice – when stand alone and when installed into the final product.
4. The CRA should **not mandate reporting of unpatched vulnerabilities**. Whilst certain disclosures may be necessary, especially when products are deployed in B2B contexts to allow mitigation measures, premature reporting of unpatched vulnerabilities across the board will open the door to even more malicious actors, jeopardising product safety with possible risks for consumers.
5. **Care should be taken in defining criticality and the content of Annex III** to ensure that the majority of products fall into the non-critical class to allow for self-assessment. Otherwise, manufacturers would pay excessive costs and the launching of new products would depend on certification processes. It is a misunderstanding that third party certification as such make products more secure as the CRA sets the same requirements on all classes. Both manufacturers and the third party notified bodies will in any case have to execute the same test according to the same standards.

We are united and stand ready in offering more insights on these topics and helping the co-legislators advance on these aspects to ensure the CRA can contribute to a stronger, more resilient Europe.

Signatories:

- APPLiA
- BSA – The Software Alliance
- Cyber Security Coalition
- DIGITALEUROPE
- Orgalim

[1] Machinery Directive (Directive 2006/42/EC) and proposed Regulation (COM(2021) 202 final).