12 July 2023

Joint Recommendations for a Feasible Cyber Resilience Act

As the EU co-legislators are making progress in setting out their positions on the Cyber Resilience Act (CRA), our associations wish to put forward concrete recommendations to support the EU's efforts to improve cybersecurity and resilience while addressing remaining criticalities in the current proposal. While both the European Parliament and the Council have made some significant improvements, many problematic aspects still need to be addressed. We therefore urge the co-legislators not to prioritise speed over quality in finalising their positions to avoid unintended outcomes.

The following recommendations aim to address key concerns shared by companies of all sizes from a variety of sectors, including software developers, device-makers, and component manufacturers. Fundamentally, more attention must be paid to **the consistency of the CRA with other applicable legislation (in particular the NIS 2 Directive and the RED Delegated Act) to avoid overlaps and duplication. When setting out the obligations under the CRA, it is also crucial to take into account international standards and existing industry best practices, as well as different business models (B2B, B2C)**. We encourage the EU lawmakers to provide proportionate and workable approaches for the following:

1. **The scope of the CRA should be clearer and narrower.**

- Any reference to "**remote data processing solutions**" should be excluded from the scope of the CRA to ensure legal clarity, and to avoid overlaps with existing legislation and unnecessary burden. **Software-as-Service, Platform-as-Service, or Infrastructure-as-a-Service should not be considered within the scope of the CRA.** We would encourage this clarification to be properly reflected in the core legal text, to provide greater legal certainty and to facilitate implementation across the EU.

- While we welcome the clarifications made regarding **open-source software (OSS)**, for legal clarity, a clear exception of OSS should be included in the core legal text. The unique characteristics of OSS must be taken into account through the entire proposal, also when creating obligations for manufacturers for OSS components that are integrated into products.

2. **There needs to be a more proportionate, risk-based approach to determining the risk level of a product with digital elements in Article 6, and greater certainty for manufacturers to ascertain if a product is a critical one.** A transparent and inclusive review process involving economic operators should be set up to determine whether a product is critical. This would avoid wrongfully designating too many products as "critical", making them more expensive, and forcing organisations to unnecessarily redirect valuable cybersecurity resources towards implementing overly stringent requirements, to the detriment of focusing on tackling real risks. For example, while the Council's approach to

simplify the criteria for allocating the products into the critical category goes in the right direction, the reference to “personal data processing” should be replaced by processing of “sensitive personal data” only, as any device today is processing personal data to some extent.

3. **Only patched vulnerabilities that have been actively exploited and pose a significant cybersecurity risk should be reported under the CRA.** Mandatory reporting of unpatched vulnerabilities represents a serious concern recently signaled by a broad industry coalition. In general, it is crucial that the reporting obligations, including the reporting timeline and the competent authority, in both Article 11(1) and (2) are in line with the NIS 2 Directive. In addition, **only “significant” incidents should be subject to the reporting obligations** of Article 11 to avoid an unmanageable reporting burden for manufacturers and responsible authorities. For the moment, the numerous amendments proposed by both legislators cannot be considered as satisfactory.

4. **Further work is needed to avoid disproportionate or impossible obligations, and obligations that would in practice increase cybersecurity risks:**

- **Annex I on essential requirements should establish proportionate obligations**. An absolute obligation to "deliver a product without known exploitable vulnerabilities" (Annex I, section I) is an impossible bar to set, as the product’s security can be influenced by numerous factors, such as the product’s deployment environment, and ignores the manufacturers' margin of action before and after a product is placed on the market. This should be **limited to any publicly known critical or highly critical vulnerabilities**.

- Similarly, determining a mandatory security update period on the basis of the “expected product lifetime” is a disproportionate and legally uncertain concept, and more clarity is needed. **Linking “expected product lifetime” solely to “reasonable user expectations”** will create great legal uncertainty across the EU single market as the actual duration periods will ultimately be determined by national market surveillance authorities and courts, not manufacturers.

- While we appreciate the improvements made so far regarding **substantial modifications** (especially on excluding security updates), further clarity and flexibility are still needed, including correlation with other relevant legislation (e.g. GPSR).

- **Compulsory differentiation between security and functionality updates is not feasible** in terms of practicality and necessary flexibility, also for the convenience of users.

- We would also welcome any changes in the CRA that recognise the difference between two categories of products – **consumer and non-consumer products**. It is key to acknowledge that in the B2B context, the buyers are organisations which have a sufficient level of cybersecurity awareness and resources to make informed purchasing decisions.

- **Also in the case of SBOMs,** the CRA should provide flexibility and consideration for best practices and international standards. For example, the Commission should work with stakeholders in developing guidance on SBOMs, instead of mandating the format and elements contained therein.

- **Provisions which would increase risks rather than improve cybersecurity**, such as **the disclosure of information on the design and development of the product** (Annex V, point 2(a)), as well as **the disclosure of details about vulnerabilities as part of an SBOM** (Annex I, Section 2, point 1), must be avoided. Similarly, **the extension of the GDPR principle of data minimisation to non-personal data** in Annex I, Section 1(3)(e), will result in poorer and stagnant experiences for users without any security benefits, as manufacturers will be limited in the collection of anonymous data that is used for quality control or track potential security threats.

- Finally, the extremely broad scope, as currently drafted, combined with the short transition period is not feasible in practice. Although the proposed amendments improve the original text, **the transition period should preferably be 72 months**, considering the entire supply chain and the need to develop standards.

We remain at the disposal of the Council and the European Parliament to provide additional information in order to find a workable solution for both businesses and users, which will increase cybersecurity.

Signatories:

BSA – The Software Alliance, https://www.bsa.org/

CCIA – Computer & Communications Industry Associations, https://ccianet.org/

Developers Alliance, https://developersalliance.org/

Information Technology Industry Council (ITI), https://www.itic.org/