CYBER RESILIENCE ACT

Ensure the cybersecurity of EV charging!

In light of the ongoing discussions on the Cyber Resilience Act (CRA), ChargeUp Europe recommends to:

- Enable manufacturers to indicate the expected product lifetime and ensure a differential treatment B2B and B2C products.
- Make more and better use of standards from compliance purposes, especially critical products.
- Ensure coherence with other digital legislation for the reporting obligations.

Introduction

ChargeUp Europe welcomes the proposal and the intention behind the Cyber Resilience Act (CRA). We share the objective of making our products more resilient and secure, not only physically but also digitally level.

The Commission's proposal could further discuss some points that would be critical to ensuring the correct and effective implementation also in the EV charging sector. As the CRA's ultimate purpose is to ensure a high level of cybersecurity of all products entering the EU market, it is necessary to consider a broader of scope of actors working on this topic.

B2B and B2C products are fundamentally different

Firstly, the legislative framework should enhance legal certainty for the economic operators placing on the market products falling under it. Therefore, the CRA should include a definition of 'product lifetime'. This would ensure that the manufacturer of the product, who is in the best position to determine the lifetime and

its capacity to provide for after-market due diligence, can plan its operations accordingly.

Most of the manufacturers in our industry operate in the business-to-business (B2B) environment, and do not supply products to the end consumer (the business-to-consumer (B2C) segment). Manufacturers' ability to provide security updates and services varies significantly in these contexts. This is especially evident given the fact that consumers do not always have specific know-how on cybersecurity, while business, depending on their size, can have different internal capacities to deal with possible cyber threats. Therefore, the CRA should differentiate between manufacturers' obligations with regards to B2B and B2C products to avoid overregulation. In addition, meeting vulnerability requirements in the B2B context largely relies on clients purchasing technical support, including product updates that remediate vulnerabilities.

Lastly, we call for the co-legislators to carefully consider the administrative burden that would result from implementing individual product conformity assessment. We recommend to lighten the administrative burden through the option of family of products assessments. Allowing one product to represent a cluster of products with similar specifications and use, the conformity assessment of that one product for presumption of conformity for the whole cluster, would be beneficial for streamlining compliance and ease the burden on smaller actors.

Standardisation as a way to facilitate compliance with the CRA requirements

Standards should be used to increase interoperability with international schemes and increase legal certainty for global actors. Relying on existing international and European frameworks would not only increase compliance but also speed up implementation.

We recommend ensuring that harmonised standards are developed based on existing frameworks and best practices as well as with industry participation.

Moreover, we welcome the intention of the co-legislators to better align the efforts on the cyber certification schemes under the Cybersecurity Act (CSA) with the compliance framework of the CRA. However, we urge to take into consideration the reality behind the time required for the issuing of such schemes and ensure that such certification can be used as a concrete tool by all actors and for all categories of products, to maximise the potential of such schemes.

We encourage the European institutions to take the long-term industry investment into account and to value it by creating a compatibility mechanism. This compatibility mechanism could take several shapes such as the referencing by harmonized standards or CSA certification scheme of already recognized industrial security standards frameworks (such as EN IEC 62443) including associated available

IACS certification schemes operated by accredited European Conformity Assessment Bodies (CAB) actors. The referred cybersecurity ecosystem also allows European industry to have an international reach and market recognition inside and outside Europe for their products with digital elements.

Lastly, common specifications should be developed under the same principles as required for the European Standardisation System (ESS): transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, and development dimension, ensuring the fair participation of all interested parties, whether public or private entities.

Alignment with other legislation to ensure a coherent reporting framework

In light of efficient and effective compliance process, the reporting obligations in CRA should be aligned with the Network and Information Security Directive (NIS2) in terms of type of incidents and timeframe. Incidents should be reported only when significant, as defined in Article 6(6) NIS2. The reporting window should be extended to 72 hours to allow adequate time for manufacturers to investigate, gather information, and respond to significant incidents while providing timely notice. This timeframe is better aligned with security objectives and internationally recognised best practices (e.g., in the General Data Protection Regulation (GDPR)).

Therefore, we recommend revising Article 11(1) to only require reporting of patched vulnerabilities, and only within 72 hours after the patch is publicly available. Additionally, the article should reference the international standard ISO/IEC 29147 as the baseline for vulnerability reporting, aligning with the EU coordinated vulnerability disclosure (CVD) framework promoted by ENISA.

Additionally, we recommend following industry best practices by establishing a model CVD policy and engaging in a deliberate campaign to encourage and track the implementation of CVD policies by economic operators. We recommend encouraging researchers to leverage CVD processes by disclosing newly discovered vulnerabilities in hardware, software, and services directly to the manufacturers of the affected product; to a national CERT, CSIRT, or other coordinator – or to a private service - that will report to the manufacturer privately.