E.DSO statement on the EU Cyber Resilience Act

E.DSO, representing Europe's leading Distribution System Operators (DSOs), welcomes the opportunity to comment on the Proposal for a Regulation on cybersecurity requirements for products with digital elements - Cyber Resilience Act (CRA). The CRA can offer a long-term solution to help manufacturers, distributors, importers, users, and authorities strengthen cybersecurity across the value chain. For this to happen, however, we must consider measures that make compliance clear and actionable rather than generate new uncertainty.

We welcome and support the proposed changes on the topic "providing security updates by manufacturers for the entire life cycle of a digital element (*not only for a maximum 5 years*)" and the consideration of the topic "Responsible Vulnerability Disclosure". Both amendments will significantly strengthen the security of Europe's critical infrastructures and we truly hope that this will also be reflected in the final version of the Cyber Resilience Act.

Having this in mind, as leading operators of critical infrastructures, we have concerns about specific provisions that could eventually lead to unnecessary expenses and the misuse of security resources. After a wide analysis conducted among DSO of various countries and dimension, we draw here some observations which are of utmost important for the Cyber Resilience Act to be promptly implemented promptly.

Article 16 of the CRA states the following	E.DSO proposal for amendment
"A natural or legal person, other than the manufacturer, the importer, or the distributor, that carries out a substantial modification of the product with digital elements shall be considered a manufacturer for the purposes of this Regulation. That person shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7), for the part of the product that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements as a whole, for the entire product."	A natural or legal person, other than the manufacturer, the importer, or the distributor, that carries out a substantial modification of the product with digital elements **and places the product on the market / makes the product available on the market** shall be considered a manufacturer for the purposes of this Regulation. That person shall be subject to the obligations of the manufacturer set out in Articles 10 and 11(1), (2), (4) and (7), for the part of the product that is affected by the substantial modification or, if the substantial modification has an impact on the cybersecurity of the product with digital elements, for the entire product."

Justification
In the case of industrial companies (operator of critical infrastructure), it is common that products with digital elements are modified by the buyer company to meet their own needs. In many cases, especially with software, it is simply necessary to adapt them to the IT and security environment. As these products are not sold on the market, but strictly for internal use, the company operating them should not be faced with obligations similar to those for placing such products on the market. As a consequence, Article 16 could lead to such a situation where the buyer companies would be obliged to fulfill the requirements of Article 10, 11 (1), (2), (4) and (7). **To mitigate such a scenario Article 16 should be limited to persons who are placing products on the market / making products available on the market.** Most of obligation set out in the above-mentioned Articles are clearly designed for products, which are sold on the market. E.g. Art. 11 (4) states: "The manufacturer shall inform, without undue delay and after becoming aware, the users of the product with digital elements about the incident and, where necessary, about corrective measures that the user can deploy to mitigate the impact of the incident." However, if a company modifies a product only for its own purposes and does not place it on the market or make it available on the market, there is no different user this company could inform. In addition, **Article 15** already covers all other economic operators who are placing the product on the market after a substantial modification (*importer and distributor*). This is already sufficient to secure the supply chain of digital products. Additional obligations for the buyer companies would not be adequate for their role and responsibilities regarding the supply chain. Furthermore, it should be clarified that there is no "*placing on the market*" / "making available on the market", if a product is only distributed within a "group of undertakings". A group of undertakings shall mean a controlling undertaking and its controlled undertakings.

E.DSO members remain at the disposal of the co-legislators to further assist in clarifying these recommendations for the success of the Cyber Resilience Act.