FEEDBACK on the

CYBER RESILIENCE ACT

Proposal for a Regulation on cybersecurity requirements for products with digital elements – 2022/0272 (COD)

The European Organisation for Security (EOS), as the representative of the European Industrial and Research Security Community, welcomes the opportunity to provide feedback to the European Commission's proposal for a Cyber Resilience Act.

EOS welcomes the introduction of essential cybersecurity and vulnerability handling requirements for products with digital elements, but stresses that further clarity is required on the scope of the Cyber Resilience Act and the relationship between the requirements it will prescribe and those found in sector-specific regulations.

To begin with, EOS views the Commission's proposal to introduce binding cybersecurity requirements for all products with digital elements at the EU level as a critical step towards strengthening European strategic autonomy and resilience. In an increasingly interconnected environment, security considerations arise from a broader range of products than those "developed exclusively for national security or military purposes" and excluded from the scope of the proposed regulation in Article 2(5). As recent events have shown, the digitalisation of supply chains and other critical infrastructures (e.g., energy 'smart grids', transport networks, communications systems etc.) – also through the use of products with digital elements – creates more entry points and vulnerabilities that malicious actors could exploit and increases the EU's exposure to risk. Robust cybersecurity standards are therefore necessary to reduce the current attack surface and promote an EU strategy against attacks with combined cyber and physical aspects. In that regard, EOS also calls on the Commission and the co-legislators to take a holistic "all hazards" approach to European security, and ensure that the proposed Cyber Resilience Act is implemented and enforced side by side with requirements around physical security – in particular when it comes to the protection of critical entities and public spaces.

EOS strongly supports the harmonisation of such standards at the EU level through this regulation to ensure that all products with digital elements in the internal market comply with the same requirements and have embedded cybersecurity by design. Given the cross-border nature of cyber threats and critical networks, an EU regulation guarantees a consistent high level of cybersecurity across Member States not only for products manufactured in the EU, but also for imported products. In that regard, EOS also supports the obligations of importers and authorised representatives enshrined in the proposal. In addition, as EOS has consistently pointed out, the adoption of common EU standards ensures a level playing field, contributes to the defragmentation of the EU market for products with digital elements and aligns practices across Member States.

For these reasons, EOS supports the strong cybersecurity by design and by default approach taken in Annex I of the proposal, as well as manufacturers' obligation to provide clear and understandable information to the user as per Annex II – which is key to ensure that end users are aware of the security features and standards of a product with digital elements before making use of it. This is again particularly important for the protection of critical entities. What is more, EOS recognises the need to match the level of cybersecurity requirements to the risks each product might entail, in particular for products used by critical entities under the recently adopted Critical Entities Resilience Directive and by essential entities under the also recently adopted NIS 2 Directive. The introduction of the categories of critical and highly critical products and the corresponding conformity assessment requirements are particularly important especially in this context, as intervention by a trusted third part is necessary to ensure compliance.

However, EOS asks for clarification on the scope of the proposal, in particular on the categories of products covered. The exception prescribed in Article 2(5) regarding products developed exclusively for national security is unclear as many such products are often used commercially as well (e.g., scanners developed for airport security). If such products are covered by the scope of the Act, there is a risk of contradiction between the requirements of the Cyber Resilience Act and those found in sector-specific regulations.
In addition, further clarity should be given in the text of the proposed regulation with regards to the harmonised standards and common specifications used to establish a presumption of conformity with the essential cybersecurity requirements. It is key for the success of the regulation that manufacturers are aware in advance of the standards and requirements they should follow during the design and productions of products with digital elements to meet their obligations under the Cyber Resilience Act. Prior to the adoption of the proposed regulation, further clarification is needed from the EU on the recognised standards for reporting, certification and disclosure to avoid a situation where manufacturers are called to comply with requirements that have not been translated into specific technical standards. Moreover, it is worth taking into consideration that additional time may be required for the implementation of the proposal and its transposition into national law, and especially for the designation or establishment of conformity assessment bodies. Industry feedback will be particularly crucial in that regard as it would help ensure that the requirements remain feasible within their proposed timeframe of adoption.

Within this approach, the close collaboration of public and private entities, including Member State authorities, industry and research centres, is a prerequisite. EOS hence encourages decision-makers to prepare the ground for European programmes aimed at promoting research initiatives to identify the appropriate standards that manufacturers should comply with to meet the essential requirements of the Cyber Resilience Act, as well as at ensuring the implementation of secure technologies, including digital products and related services, in European infrastructure.

10 January 2023