European Economic and Social Committee

OPINION

European Economic and Social Committee

Cyber Resilience Act

Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020
[COM(2022) 454 final – 2022/0272 (COD)]

INT/999

Rapporteur: **Maurizio MENSI**
Co-rapporteur: **Marinel Dănuț MUREȘAN**

Referral	European Parliament, 09/11/2022
	Council of the European Union, 28/10/2022
Legal basis	Article 114 of the Treaty on the Functioning of the European Union
Section responsible	Single Market, Production and Consumption
Adopted in section	10/11/2022
Adopted at plenary	14/12/2022
Plenary session No	574
Outcome of vote (for/against/abstentions)	177/0/0

1. Conclusions and recommendations

1.1 The EESC welcomes the Commission's proposal for a Cyber Resilience Act (CRA) aimed at setting higher cybersecurity standards and thus creating a reliable system for economic operators while guaranteeing EU citizens that all products on the market can be used safely. This initiative forms part of the European data strategy, which strengthens the security of data, including personal data, and fundamental rights, which are essential requirements for our digital society.

1.2 The EESC considers it essential to strengthen the collective response to cyber attacks and to consolidate the process of harmonising national-level cybersecurity in terms of operational rules and tools, to prevent different national approaches creating legal uncertainties and obstacles.

1.3 The EESC welcomes the Commission's initiative, which will not only help to reduce the significant costs for businesses caused by cyber attacks, but will also enable citizens/consumers to benefit from better protection of their fundamental rights, such as privacy. In particular, the Commission shows that it is taking account of the specific needs of SMEs when it comes to the services provided by the certification authorities; however, the EESC points to the need to clarify the criteria that apply here.

1.4 The EESC considers it important to point out that, while it is commendable that the CRA covers virtually all digital products, the practical application of the CRA might be problematic given the considerable and complex monitoring and oversight it entails. Hence the need to strengthen the monitoring and oversight tools.

1.5 The EESC points to the need to clarify precisely the material scope of the CRA, with particular reference to products with digital elements and software.

1.6 The EESC notes that manufacturers will be obliged to report both vulnerabilities in their products and any security incidents, informing the EU Agency for Cybersecurity (ENISA). In this regard, it will be important that ENISA be provided with the necessary resources to carry out effectively and in a timely manner the important and sensitive tasks entrusted to it.

1.7 To avoid any uncertainty when it comes to interpretation, the EESC suggests that the Commission draw up guidelines to guide manufacturers and consumers on the exact rules and procedures that apply in practice, since it appears that a number of products within the scope of the proposal are also subject to other legislation on cybersecurity. In this regard it would be also important that in particular SME and MSME have access to qualified expert support, able to provide specific professional services.

1.8 The EESC notes that the relationship between the certification authorities under the CRA and other bodies authorised to certify cybersecurity under other legislation is not entirely clear. The same problem may also arise when it comes to operational coordination between the surveillance authorities provided for in this proposal and those already operating in accordance with other legislation applicable to the same products.

1.9 The EESC points out that, under the proposal, the certification authorities will have to shoulder a considerable amount of work and responsibility. It must be ensured that they are fully operational in practice, not least in order to prevent the CRA adding to the existing administrative burden and thus penalising manufacturers that will have to comply with a number of additional certification requirements to be able to continue to operate on the market.

2. Analysis of the proposal

2.1 With the proposal for a CRA, the Commission is seeking to rationalise and reshape the current cybersecurity legislation in a comprehensive and cross-cutting manner, while updating it in the light of technological innovations.

2.2 The CRA essentially pursues four objectives: ensure that manufacturers improve the security of products with digital elements at the design and development phase and throughout the whole life cycle; ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers; enhance the transparency of the security properties of products with digital elements; and enable businesses and consumers to use these products securely. In essence, the proposal introduces a CE marking for cybersecurity, which is to be affixed to all products covered by the CRA.

2.3 This is a horizontal intervention, through which the Commission intends to regulate the whole area in a systemic way, as it covers virtually all products with digital elements. It excludes products of a medical nature, products related to civil aviation, vehicles and products for military purposes. The proposal also excludes SaaS (cloud) services, unless they are used to develop products with digital elements.

2.4 The definition of "products with digital elements" is very broad and includes any software or hardware product, as well as software or hardware not embedded in the product but placed on the market separately.

2.5 The legislation introduces mandatory cybersecurity requirements for products that have digital elements, covering their entire life cycle, but does not replace those already in place. Rather, products that have already been certified as complying with pre-existing EU standards will also be considered "valid" under the new Regulation.

2.6 The basic general principle is that only "secure" products are placed on the market in Europe, and that their manufacturers ensure that these products remain secure throughout their life cycle.

2.7 A product is considered "secure" if it is designed and manufactured in such a way that it has a level of security appropriate to the cyber risks that its use entails, has no known vulnerabilities at the time it is sold, has a secure default configuration, is protected from unlawful connections, protects the data it collects, and ensures that the data collected is limited to what is needed for its operation.

2.8 A manufacturer is considered fit to place its products on the market if it makes available a list of the various software components in its products, quickly issues remedies free of charge in the event of new vulnerabilities, makes public and details the vulnerabilities it detects and resolves, and regularly checks the "robustness" of the products it places on the market. These actions and the other requirements imposed by the CRA must be carried out throughout the product's life cycle, or for at least five years after it has been placed on the market. The manufacturer is required to ensure that vulnerabilities are eliminated through regular software updates.

2.9 In accordance with a general principle applied in various sectors, the obligations are also imposed on importers and distributors.

2.10 The CRA provides for a "default" category of products and software for which a self-assessment by the manufacturer can be relied upon, as is already the case for other types of CE marking certification. According to the Commission, 90% of the products on the market fall within this category.

2.11 The products in question may be placed on the market following a self-assessment of their cybersecurity by the manufacturer, which must provide the appropriate documentation established in the regulatory guidelines. The manufacturer is required to repeat the assessment if the product is modified.

2.12 The remaining 10% of products are divided into two other categories (Class I, lower-risk, and Class II, higher-risk), which require more vigilance when placed on the market. These are known as "critical products with digital elements", the failure of which can lead to other dangerous and wider security breaches.

2.13 For products in these two categories, the basic self-assessment is only permitted if the manufacturer demonstrates that it has complied with specific market standards and security specifications or cybersecurity certification schemes already provided for by the EU. If that is not the case, it may obtain product certification from an accredited conformity assessment body, and this is mandatory for Class-II products.

2.14 Such a system for classifying products in risk categories is also contained in the Proposal for a Regulation on AI (artificial intelligence). To avoid doubts about the applicable provisions, the CRA covers products with digital elements that are simultaneously classified as "high-risk AI systems" under the AI proposal. Such products will generally have to comply with the conformity assessment procedure set out in the AI Regulation, except for "critical products with digital elements", for which the CRA's conformity assessment rules will apply in addition to the CRA's "essential requirements".

2.15 In order to ensure compliance with the CRA, each Member State is to designate a national authority to carry out market surveillance. In line with the legislation regarding the safety of other products, if a national authority finds that a product's cybersecurity features are no longer valid, it may be withdrawn from the market in the State in question. ENISA has the power to carry out detailed evaluations of notified products, and its evaluations, where a product is found to be unsafe, may lead to it being withdrawn from the EU market.

2.16 The CRA includes a series of penalties – corresponding to the seriousness of the infringement – which, in the event of a breach of the essential cybersecurity requirements for these products, can amount to EUR 15 million or 2.5% of turnover for the preceding financial year.

3. Comments

3.1 The EESC welcomes the Commission's initiative aimed at inserting a key element into the wider patchwork of cybersecurity regulation, in coordination with and in addition to the NIS Directive and in addition to the Cybersecurity Act. High cybersecurity standards have a key role to play in creating a robust EU cybersecurity system for all economic operators, aimed at guaranteeing EU citizens that all products on the market can be used safely and increasing their confidence in the digital world.

3.2 The Regulation therefore addresses two issues: the low level of cybersecurity of many of the products and, above all, the fact that many manufacturers do not provide updates to address vulnerabilities. While manufacturers of products with digital elements sometimes suffer reputational damage when their products fall short on security, the cost of the vulnerabilities is mainly borne by professional users and consumers. This reduces the incentive for manufacturers to invest in the design and development of secure products and to provide security updates. Moreover, businesses and consumers are often insufficiently and inaccurately informed when it comes to choosing secure products and often do not know how to make sure that the products they buy are securely configured. The new rules address these two issues by tackling the question of updates and the provision of up-to-date information to customers. The EESC believes that, in this sense, where properly applied, the proposed regulation could become an international benchmark and model for cybersecurity.

3.3 The EESC welcomes the proposal aimed at introducing cybersecurity requirements for products with digital elements. It will be important, however, to avoid overlaps with other existing regulatory provisions on this issue, such as the new NIS 2 Directive and the AI Act.

3.4 The EESC considers it important to point out that, while it is commendable that the CRA covers virtually all digital products, the practical application of the CRA might be problematic given the considerable monitoring and oversight it entails.

3.5 The material scope of the CRA is broad and covers all products with digital elements. According to the proposed definition, all software and hardware products and related data processing solutions are covered. The EESC suggests that the Commission clarify whether all software falls within the scope of the proposed regulation.

3.6 Manufacturers will be obliged to report both actively exploited vulnerabilities and security incidents. They will be required to inform ENISA of any actively exploited vulnerabilities contained in the product and (separately) of any incident that has an impact on product security, in both cases within 24 hours of becoming aware of it. The EESC points here to the need for ENISA to be provided with sufficient resources – both in numerical terms and in terms of

professional training – if it is to be able to carry out effectively the important and sensitive tasks entrusted to it under the Regulation.

3.7 The fact that a number of products falling within the scope of the proposal are also subject to other cybersecurity legislation might lead to uncertainty as to which rules apply. Although the CRA is designed to be consistent with the current EU product regulatory framework and other proposals currently in the pipeline under the EU Digital Strategy, rules such as those for high-risk AI products, for example, overlap with those in the Regulation on the processing of personal data. In this regard, the EESC suggests that the Commission draw up guidelines for manufacturers and consumers on how it should be applied correctly.

3.8 The EESC notes that the relationship between the certification authorities under the CRA and any other bodies authorised to certify cybersecurity under other equally applicable regulations does not seem entirely clear.

3.9 In addition, those certification authorities will have a considerable burden of work and responsibility. It must be verified and ensured that they are fully operational in practice, in order to prevent the CRA leading to an increase in the administrative burden already imposed on manufacturers operating on the market. In this regard it would be also important that in particular SME and MSME have access to qualified expert support, able to provide specific professional services.

3.10 The CRA requires the certification authorities to take into account the specific needs of SMEs when performing their services; however, the EESC points to the need to clarify the criteria that apply here.

3.11 A problem may also arise when it comes to coordination between the surveillance authorities provided for in this Regulation and those already operating in accordance with other rules applicable to the same products. The EESC therefore suggests that the Commission call on the Member States to monitor the situation and, where appropriate, take action to prevent this happening.

Brussels, 14 December 2022.

Christa SCHWENG
The president of the European Economic and Social Committee