SVENSKT NÄRINGSLIV

Finansdepartementet

i.remissvar@regeringskansliet.se
i.esd@regeringskansliet.se

Our reference number:
SN 2022-157

Your reference number:
I2022/01758

2023-02-21

Consultation Response

Regarding the European Commission's proposal for a regulation of comprehensive cybersecurity requirements for products with digital elements and for the amendment of Regulation (EU) 2019/1020

The Confederation of Swedish Enterprise would like to express the opinion that:

1. It is important that the proposal is based on the New Legislative Framework (NLF) and that self-assessment of conformity can be performed for as many products as possible.

2. The scope of the proposal is important for the cyber resilience of products, but the exception for Software as a Service (SaaS) and remote data processing needs to be clarified. Exclude hardware, software and services used for the processing, transmission and storage of remote data to avoid duplication with NIS2 ((EU) 2022/2555).

3. A risk-based approach is of central importance and must be based on the intended use of the product. This applies, for example, to vulnerability requirements, vulnerability management and vulnerability reporting. Compliance with at least two of the criteria set out in Article 6.2 a shall be required. Article 6.2 b shall be deleted. The requirements shall be limited to vulnerabilities that are critical or significant according to definitions established in existing standards such as Common Vulnerability Scoring System (CVSS). The risk assessment that is already required for all products that are self-validated according to NLF, should be advantageously used.

4. Notification of incidents and vulnerabilities needs to be extended beyond 24 h and comply with corresponding requirements in, for example, NIS2 and GDPR (72 h). The obligation to notify should be limited to a significant incident or incident leading to a significant cybersecurity risk.

Svenskt Näringsliv Confederation of Swedish Enterprise
Postadress/Address: SE-114 82 Stockholm Besök/Visitors: Storgatan 19 Telefon/Phone: +46 (0)8 553 430 00
svensktnaringsliv.se Co. reg. no.: 802000-1858

5. Market-driven international standards and harmonised standards provide predictability and competitiveness. In addition, they are central not least to SMEs' ability to comply with regulations and conformity assessment (self-validation). Self-validation in turn is important to avoid bottleneck problems in third-party assessments. Common specifications should not be used.

6. The implementation of the proposal needs to be extended to 48 months in order to give manufacturers a reasonable time and opportunity to meet all the requirements of new comprehensive and sectoral legislation. 48 months is also a realistic implementation period for both harmonised standards to be put in place and then used by companies in the self-assessment of conformity.

PRELIMINARY REMARKS

One of the goals of CRA is to create competitive advantages for companies in Europe. To achieve that goal, unnecessary bureaucracy and burden must be avoided. The proposal needs to be combined with strengthened cybersecurity risk management, adequate competence and secure and robust infrastructure. The new laws adopted under the EU's cybersecurity strategy will deliver results, but will also have an impact on the capacity of both companies and regulators.

In order to attain legislation that reduces cybersecurity incidents with an impact on the security of a product, it must be applicable in different contexts. For example, vulnerabilities differ significantly depending on whether it concerns telecom networks, companies, or consumers' management of IoT products. The Confederation of Swedish Enterprise therefore wants to emphasize the need for proportionate legislation with a risk-based method. Security efforts must focus on addressing critical and serious vulnerabilities. The focus should therefore be on minimising cyber incidents and not on minimising the occurrence of all forms of vulnerability.

Furthermore, Europe should make maximum use of international standards and market-driven initiatives to strengthen competitiveness. Therefore, future harmonised standards should, as far as possible, be based on existing international standardisation work and agreements on mutual recognition should be sought with third countries. Cybersecurity is a global challenge, a continuous process and not a solid state in a product.

The Confederation of Swedish Enterprise agrees that cybersecurity needs to be strengthened in society and companies will contribute to a large extent. Not least with the NIS2 directive, where the requirements are increasing significantly for many companies. Authorities working with Cybersecurity need to support the work of companies through information sharing and transfer of knowledge. The National Cyber Security Centre should urgently strengthen collaboration with the business community by the development of routines for communicating situational awareness and information on the management of cyber-attacks.

BALANCED PROVISIONS

In many ways, the comprehensive approach based on the NLF will facilitate compliance. This well-functioning regulatory process makes it possible to cover different levels of necessary protective measures, based on the risk profile of the products and their intended application.

We welcome the clarification in Article 16 that a substantial modification of a product made by a natural or legal person (other than a manufacturer, importer or distributor) is subject to obligations. This is an important element because it leaves it up to the natural or legal person to choose how they want to use and modify their product, and even potentially market it as a new product.

For reasons of competition, it is essential and welcome that notified bodies apply conformity assessment procedures without creating unnecessary burdens for economic operators, in line with the intention of Article 37.

The open market economy makes it possible to sell European products outside the EU as well as to import products from third countries. This gives customers choice and healthy competition. It is therefore essential that mutual recognition agreements with third countries on conformity assessment can be concluded for the products covered by the proposal. This will facilitate trade and strengthen cybersecurity in the single market and globally. The internal market also relies on an effective standardisation system, which should be aligned with international standards to enable trade, cooperation, and interoperability within and outside the Union.

SUGGESTIONS FOR IMPROVEMENTS

The Confederation of Swedish Enterprise believes that legislators should focus on further clarifying definitions, scope, risk categorisation and consistency with other rules.

SCOPE OF APPLICATION AND DEFINITIONS

Consistency of definitions is very important. In Article 3, the definition of ‘product with digital components’ needs to be clarified. The CRA alone distinguishes between four types of products with digital elements: i) products with digital elements; ii) Class 1 critical products with digital elements; iii) Class 2 critical products with digital elements; and iv) highly critical products with digital elements. It is apparent that this differentiation aims at better risk categorisation and product identification, but this is insufficient to provide the clarity needed to avoid overlaps or confusion with NLF-based regulations to be negotiated or applied in parallel, such as the AI Act and the Machinery Regulation.

In addition, Article 3.1. clearly defines ‘products with digital elements’ as ‘any software or hardware product and its remote data processing solutions, including software or hardware components, to be placed on the market separately’. However, recital 9 states that the proposal does not cover software as a service (SaaS) except ‘for remote computing solutions’.

The Confederation of Swedish Enterprise advocates excluding software as a service (SaaS), given that

i) NLF has not been applied to services and it will become a new area, and
ii) The NIS2 Directive already imposes an obligation on cloud service providers (including SaaS) to implement cyber and risk management measures, as they are considered as providers of essential services.

The exclusion of open-source software that is not used in connection with commercial activities also needs to be clarified. Recital 10 sets out what is to be understood as the commercial activity of software, but extends it to technical support services, which appear to include SaaS. Here clarification or guidance is needed on how the liability requirements for open source software components can be implemented in software. Open source software should be handled in a consistent manner whether or not it is linked to a commercial activity.

The definition of ‘substantial change’ should be in line with the Blue Guide (2022) and the recently revised Machinery Regulation. To this end, recital 22 should be adapted to Article 3.31

It should be avoided that each software release requires the product to undergo a new conformity assessment, as this would place a disproportionate burden on the developer and also delay the updates. The Blue Guide makes it clear that material changes must be assessed on a case-by-case basis, but for CRA's large scope of products, this may not be technically feasible?

The concept of releasing a product on the market ‘without any known exploitable vulnerability’ is not risk-proportionate, as maintaining an adequate level of cybersecurity is a process that must be risk-based. In addition, a product's cyber resilience and thus the existence of a vulnerability can be affected by many factors, including the product's distribution environment. For example, compare the difference in environment of consumer products or B2B system solutions.

All vulnerabilities have the same impact and do not represent a significant cybersecurity risk as defined in Article 3.36. In line with the OECD findings, there is no way to eliminate all vulnerabilities. While it is important to address vulnerabilities, it would not be a realistic goal to address all vulnerabilities due to cost and technical feasibility. Therefore, the aim should be to minimise cyber incidents by addressing the critical vulnerabilities (scored by e.g. the globally recognised CVSS system standard).

Action in the form of a security update is a reasonable expectation, but performing a demanding update free of charge for complex products and systems is contrary to current industry practice. In consumer environments, users accept that an update will result in devices being unavailable, which is not the case for many critical infrastructures. Therefore, the proposal should be proportionate and avoid a blanket introduction of free updating. In point 8 of Annex 2, Section 2, ‘free of charge’ should be complemented by ‘free of charge or at a fair, transparent and non-discriminatory cost’, which has been used in Regulation (EU) 2019/424 on ecodesign requirements for servers and data storage products. This would be in line with existing industry practice for security updates in complex products without the risk of fragmenting the market.

In addition, it is almost impossible to decouple security updates from regular software upgrades in the context of complex systems and networks, as opposed to consumer products. See Annex 1, Section 1, point 3 k.

RISK CATEGORISATION AND COMPLIANCE
Focuses on the intended use of products. This is necessary because a product may perform a more critical or less critical function depending on the specific application environment. For example, from the industry's point of view, whether the same microprocessor is used in a coffee machine, or a router makes a significant difference in terms of criticism.

In simple terms, the proposal divides products with digital elements into two categories. A larger group where manufacturers can self-validate whether products meet cybersecurity requirements. The second group consists of critical products with digital elements, whose compliance must be assessed by a third party. **Article 6** sets out in more detail what must be taken into account for a **product to be considered critical.** For the article to be relevant, a risk-based assessment is needed, the scope limited and clarified. For example, it is unreasonable to consider all products used in industrial environments (see paragraph 2 point b) to be critical.

A wide range of products are covered by CRA and the capacity for third-party conformity assessment can create significant bottlenecks and workload for both companies and assessment bodies.

European and national regulators are currently implementing or not yet transposing a very broad regulatory framework for cybersecurity (NIS2, DORA, sector-specific rules). Within the foreseeable future product-specific cybersecurity certification schemes, stemming from the Cybersecurity Act (e.g. Cloud Scheme (EUCS) and 5G Scheme (EU5G)). It is therefore very important to avoid any form of overlap or inconsistency in legislation. To this end, we strongly recommend that ENISA and the Commission limit the development of new cybersecurity certification schemes under the Cybersecurity Act (CSA) to what is absolutely necessary.

In addition, to ensure legal clarity, the cybersecurity requirements of a harmonised standard must take precedence if there is a conflict between the CRA and another (existing) legislation.

Although the drafting of common specifications in Article 19 is intended as a fall-back measure, it is not clear that it is necessary at this stage to have such a possibility at all within the first comprehensive legislation on cybersecurity requirements for products. Deleting this option will strengthen the incentive for the market to develop standards that are agile and result-oriented, in particular with regard to meeting the comprehensive requirements of this Regulation.

COMPLIANCE WITH OTHER LEGISLATION
It is essential that the CRA does not lead to an overlap of cyber requirements for a particular product. A product, given a specific application, should be subject to a set of cybersecurity requirements. It is the Commission's intention to maintain substantially equivalent requirements for products in the General Product Safety Regulation (GPSR), the AI Act and the Machinery Regulation (MR) in relation to the CRA. We propose that only the CRA be applied to the products covered by the aforementioned regulations. In addition, new *lex*

specialis should always be based on the same principles as the CRA.
The CRA includes reporting mechanisms that will lead to faster action for the products concerned. However, it must be stressed that reporting is a burdensome task, as it is time-consuming to collect information. Incident management and actions must be a priority. Reporting requirements should be in line with the NIS2 Directive and GDPR and adjusted to 72h.

In the case of vulnerability notifications, it should be noted that a vulnerability can be actively exploited for several months without the manufacturer being aware of it. Or a vulnerability can be identified months after an incident had occurred. Alignment with the NIS2 Directive is therefore necessary, in particular in view of ENISA's forthcoming vulnerability database, the voluntary publication of vulnerabilities foreseen in the revised Directive and the information in the final report following an incident, which will also describe the vulnerability that led to it. Companies should not be obliged to report the same information several times.

The vulnerability reporting obligation is limited to those vulnerabilities that are ‘actively exploited by a malicious actor’, pose a ‘significant cyber risk’ and ‘a high risk to the functioning of the internal market’. In addition to the changes to Article 11, recital 34 needs to be amended as it states that 'any exploited' vulnerability should be considered a threat to the internal market, which is disproportionate and not in line with the risk-based approach used throughout the CRA Regulation.

Mandatory vulnerability reporting shall follow established principles for responsible coordinated disclosure of vulnerabilities. Establish a vulnerability risk assessment system based on objective criteria and in synergy with established scoring methods such as CVSS. Taking action too early can have a negative impact and lead to greater cyber exposure and less resilience.

The primary objective of EU cyber resilience efforts should be to support market actors and enable the rapid mitigation of an incident or actively exploited vulnerability by a malicious actor that poses a significant cyber risk.

To meet the security objectives of the proposal, the right balance is needed between enabling the necessary exchange of information between manufacturers and regulators, without further exposing products to malicious attacks by requiring disclosure of the vulnerability when fixes are not available.

A fully digital flow of information and secure reporting must be established both to ENISA and between ENISA, national competent authorities and market surveillance bodies- Manufacturers of products with digital elements should only have to report once within the EU Effective reporting mechanisms that ensure the one-time principle for data disclosure are crucial for companies to be able to focus their time on incident and vulnerability management and not on reporting the same information to different national and EU institutions.

CONFEDERATION OF SWEDISH ENTERPRISE

Carolina Brånby