LEWIATAN

Warszawa, 20 października 2022 r.
KL/412/200/AM/2022

Pan
Janusz Cieszyński
Pełnomocnik Rządu ds. Cyberbezpieczeństwa
Sekretarz Stanu ds. Cyfryzacji
Kancelaria Prezesa Rady Ministrów

Szanowny Panie Ministrze,

W nawiązaniu do zaproszenia do konsultacji *Cyber Resislience 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*), Konfederacja Lewiatan, w załączeniu, przekazuje stanowisko do projektu.

Z poważaniem,

Maciej Witucki
Prezydent Konfederacji Lewiatan

Do wiadomości:
Pan **Łukasz Wojewoda**
Dyrektor Departamentu Cyberbezpieczeństwa
Kancelaria Prezesa Rady Ministrów

Pani **Katarzyna Prusak – Górniak**
Radca**,** cyber attaché
Stałe Przedstawicielstwo RP przy UE w Brukseli

Załącznik: Stanowisko Konfederacji Lewiatan do projektu rozporządzenia *Cyber Resislience Act*

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

Stanowisko Konfederacji Lewiatan do projektu rozporządzenia *Cyber Resislience Act*

I. General comments.

1.1. Powers to act against compliant products across EU 27 states

Article 46 of the CRA specifies a procedure whereby Member State authorities can remove compliant products from the market. The Commission will have to be notified and will trigger a process of risk assessment (with the help of ENISA) that could result in the removal of compliant products if they have "significant cybersecurity risk" and pose a risk to NIS2 entities or "public interest protection." There are serious concerns regarding the definitions of significant cybersecurity risk' concerning critical products (defined in NIS2 concerning non-technical factors). We see the risk of fragmentation of the single market, given that a non-binding political document (5G toolbox) was used as a benchmark for risk assessment and led to similar results. We also want to note that fewer vendors on the EU market will reduce cybersecurity as vendor diversity makes it difficult for attackers to compromise vulnerabilities (see recital 58). We strongly support the free market as the best tool to ensure that the products are secure and not vulnerable.
Eliminating a significant supplier can also cause negative downstream effects such as (i) lack of cooperation on interoperability testing, (ii) price predation to lock in customers and (iii) exclusivity or most-favored-nation clauses in contracts with subcontractors.

1.2. Relation to NIS2 (non-technical requirements)

NIS2 and the CRA are closely linked because the products used by "critical infrastructure operators" under NIS2 also are in scope in CRA (see art. 6 p. 2 letter (b) CRA). However, any essential requirements in NIS2 and CRA should be based on the risk assessments of the technical risk factors, not by undue influence by a third country on suppliers (see recital 33). Any requirements should not lead to delays or encourage discrimination of vendors based on politicized needs – such provisions should not be based on country of origin but rather focus on the product or device itself. Relying on not clear, vague, and highly political criteria may lead to a lower innovation pace. The idea of political assessment is also reflected in Art. 46, which refers **to products that present a "significant cybersecurity risk" despite being compliant** when "the availability authenticity, integrity or confidentiality of services offered using an electronic information system by essential entities of the type referred to in [Annex I of (NIS2)] or to other aspects of public interest protection. We want to stress that reliance on political criteria will lead to decreased fair competition and level of security. Any such criteria may result in using devices or products far less secure from the vendor from a "politicly scrutinized" country. It is also recommended to remove references to EU Toolbox on 5G cybersecurity in recital 33 as it relates to the soft law. We understand that politics and

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

economic interests should be essential to the legislation. Still, the European Union has already implemented several tools that enable dynamic and flexible activity (see Regulation (EU) no 833/2014 concerning restrictive measures or eight packages of sanctions against Russia).

1.3. Overlapping requirements

The CRA offers the possibility of reducing complexity between different, often sectoral, regulatory approaches to the cyber security of products and harmonizing the regulatory landscape under a single, horizontal, consistent, and coherent reference point.We want to point out that it is necessary to clarify relationships and links between CRA and cybersecurity certification under the Regulation (EU) 2019/881 (Cybersecurity Act), AI Act, eIDAS Regulation, and DORA. All of these acts should enable harmonization and interoperability. Even for large entities, it is becoming harder and harder to identify and assess all the impacts of different regulations. This could lead to massive interoperability of systems and products across UE and non-compliance risk for manufacturers and vendors.
Apparent example of overlapping is Article 6 (a) and (5b) of the CRA. Essential entities under NIS2 using digital products in their supply chain will have to comply with requirements in the CRA. At the same time, NIS2 requirements would be prioritized, and therefore scope for fragmentation remains.
CRA should use a collaborative approach to everyday challenges, enabling global cooperation and interoperability. Support a reduction of complexity between different sectoral regulatory policies through horizontal regulation and using harmonized international standards in EU product rules under the New Legislative Framework. If national standards exist, they should be aligned with international standards. As ICT standardization is already global in nature, an existing standardization infrastructure can be used with the involvement of all stakeholders (ISO/IEC JTC1, CEN/CLC/JTC 13, ETSI TC CYBER).

1.4. Scope of the Regulation

We believe that the scope of the regulation is too extensive and includes software, hardware, and components. In a time of rising prices, there is a balance or trade-off to be struck between higher security and better efficiency in the market (see art. 3 (1), (3), (4), (14) of the CRA). Arbitrary enforcement and the burden on the industry could have knock-on effects on prices and economic costs. We also identify that the list of critical products (class 2) in Annex 3 should be narrowed, as is, to very general categories of products (e.g., *operating systems for servers, desktops and mobile devices, Routers, modems intended for the connection to the internet, and switches, intended for industrial use*)
We identify onerous obligations on products, including new standards and requirements like Software Bill of Materials (SBOM – see. Art. 3 (37) of the CRA), as well as on vulnerability

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

handling and incident reporting (specifically clarification of definitions and setting reasonable and non-overlapping requirements). Requirements have to be proportional and increase business and legal certainty (see recital 37, 63 and article 3 (37(and Article 11). We would also like to note that the wording relating to SBOM in Annex I p. 2 Vulnerability Handling Requirements should be removed.

1.5. Scope of the critical products, categories, and specifications (requirement to enshrine non-discrimination and ensure a level playing field for non-EU vendors)

Article 6 (2a) CRA gives the Commission delegated act powers to include a new type in the list of categories of critical products or withdraw an existing one. The Commission needs to determine the level of cybersecurity risk to do this and can use the following criteria: (i) it is designed to run with elevated privilege or manage privileges; (ii) it has direct or privileged access to networking or computing resources; (iii) it is designed to control access to data or operational technology; (iv) it performs a function critical to trust, in particular security functions such as network control, endpoint security, and network protection. Article 6 (2e) also specifies that the extent to which the use of products with digital elements has already caused material or non-material loss or disruption or has given rise to significant concerns concerning the materialization of an adverse impact is a criterion to add or remove products. Such powers allow the European Commission to extend the scope of CRA without any control. It would be better to have a broader scope of the regulation instead of the content, which may be changed at any time. Such an approach will reduce uncertainty crucial in the R&D, innovative, and digital sectors.
We want to point out that the EU legislator use very vague provisions, e.g., "concerns" or "elevated privileges," and "significant concerns," which may lead to different interpretations and discretional powers not limited by standard democratic mechanisms. The Commission has given itself powers in Article 6 to extend the scope of critical products using criteria that includes products that have "given rise to significant concerns" (high capacity for politicization), as well as products in "industrial settings" (pick and choose scope). The same concerns arise in article 6 (2e), where EU legislator uses "significant cybersecurity risk' regarding critical products (defined in NIS2 concerning non-technical factors). Such general proviso may lead to single market fragmentation.

1.6. Conformity assessment

In our view, the manufacturers should be able to decide their appropriate levels of assurance, and all the assurance should be based voluntarily. We stand by the position that it is up to the manufacturers themselves to adapt to safety requirements - of which the free market will always be a reliable verifier. Of course, we do not question the need to

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

implement specific standards at all, but they should not be as broad as those adopted in the CRA. Any higher conformity assessment requirements should only be technical.

1.7. Full lifecycle requirements

We are concerned that requirements, including the entire product lifecycle, may lead to economic inefficiencies. The manufacturers will invest a significant amount in ensuring a proper level of security during the whole lifecycle of the product instead of concentrating on innovation. It is essential that the duration of the life cycle is defined by the manufacturer and communicated transparently to the users. Essential to establish self-assessment as a standard conformity procedure. Additional compliance costs should be as low as possible and not lead to new legal uncertainty in businesses.

1.8. Powers to influence and shape conformity assessments

Article 6 (5) of the CRA gives the Commission delegated act powers to specify categories of highly critical products for which the manufacturers will be required to obtain a European cybersecurity certificate under a European cybersecurity certification scheme according to CSA (2019/881) to demonstrate conformity with the essential requirements. When determining such categories, the Commission will consider (1) whether entities in NIS2 will use it or will use it in the future and (2) whether it is relevant for the resilience of the supply chain. However, we would like to propose that in the absence of relevant specified schemes, the European Commission should lean on international standards and schemes (e.g., ISO). This language should be added, even for critical products.
We would also like to propose that article 18 p. 4 of the CRA European Commission should be empowered to require manufacturers to produce an EU cybersecurity certificate in cases where there is an exemption for third-party conformity assessment and then decide whether this is inadequate (see recital 39).

II. Key recommendations

We have provided the following key recommendations that we believe should be implemented to improve the proposed regulation:

1. Reduce powers to extend the scope of critical products: Sharpen language:
    a. **Article 6 (2):** "significant concerns in relation to the materialization of an adverse impact" – very vague and general with a disproportionately broad remit and toolkit of measures. Suggest deletion of the last part of (e): "significant concerns."

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

b. **Article 6:** Without relevant specified schemes, the European Commission should lean on international standards and schemes (e.g., ISO), and this language should be added, even for critical products.

c. **Article 6:** The European Commission has given itself powers to extend the scope of critical products using criteria that includes products that have "given rise to significant concerns" as well as products in "industrial settings." Such broad delegation should be removed.

d. **Chapter II:** Manufacturers should decide through self-assessment on appropriate measures. Add text on non-discrimination.

e. **Article 46:** Ensure this is proportionate and limit the European Commission's vast discretionary powers that increase cybersecurity's politicization.

2. Re-examine ability to remove compliant products from the market:

a. CRA includes a mechanism for the Member States and the Commission to trigger a process to remove products that are compliant with the regulation if they have "significant cybersecurity risk" and pose a risk to NIS2 entities or "public interest protection." EU institutions should add safeguards and make this mechanism proportionate and non-discriminatory.

3. Wide scope creates market inefficiencies and adds costs:

a. In a time of rising prices, there is a balance or trade-off to be struck between higher requirements and better efficiency in the market. Arbitrary enforcement and the burden on the industry could have knock-on effects on prices and economic costs. A wide scope will add burdens on SMEs and industry, and this is why requirements should be minimized, with all manufacturers able to self-assess their respective levels of assurance. In case wide scope needs to be maintained, it should be aligned with the Cybersecurity Act (CSA).

4. Static requirements reduce vendor diversity and cybersecurity:

a. Static criteria like those based on "country of origin" opens the door for requirements that could be subject to political interpretation by the Member States. The 5G toolbox contributed to not only fragmentation but also discrimination based on country of origin and does not comply with good governance or principles of EU law. This reduces vendor diversity and makes the EU less safe as a result.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

5. Reduce uncertainty in conformity assessment:

   a. Commission should allow both EU cybersecurity schemes and self-declaration of conformity with similar or equivalent international standards. European Commission can require manufacturers to produce an EU cybersecurity certificate instead of an exemption for third-party conformity assessment (Class I) and still decide whether this is adequate.

   b. **Article 24:** Legal uncertainty in the definition of "critical products" as the link to NIS2 makes it unclear which products will require high assurance (third-party conformity assessment). In addition, the European Commission has given itself powers to define additional product categories in the scope, as well as new

6. Minimize requirements on developers, startups, SMEs, etc.:

   a. While SMEs should implement equally high-security requirements, it is essential to provide support to allow them to compete. Critical to avoid excessively prescriptive technical requirements and maintain the horizontal character of the CRA while also removing all scope for the Member States to include non-technical criteria. Another solution is to avoid the inclusion of non-critical or standalone software.

7. Re-examine the link to NIS2:

   a. In light of distortions to the single market caused by NIS2 implementation; it is prudent to reconsider the inclusion of Article 6 para 5 altogether. It is suggested to delete this additional concept of "highly critical products." Essential entities under NIS2 using digital products in their supply chain will have to comply with requirements in the CRA. At the same time, NIS2 requirements would be prioritized and so the scope for fragmentation remains. This will add uncertainty and a political dimension to risk assessment.

8. Preserve the Brussels effect:

   a. EU has traditionally set global technology standards by allowing all stakeholders to have influence in a structured way that respects neutrality and the rule of law. Under the proposal, European Commission could specify new categories of products to the scope and use flexible criteria to justify decisions, for e.g., "given rising to significant concerns related to the materialization of adverse impact." Link to the 5G toolbox means the further scope for unjustified politicization. Exclusion and unjustified politicization only reduce strategic autonomy and harms the EU's leadership as a rule-

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS

LEWIATAN

setter. Instead, link to international standards, conduct impact assessments and improve transparency.

KL/412/200/AM/2022

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel.(+48) 22 55 99 900
fax (+48) 22 55 99 910
lewiatan@konfederacjalewiatan.pl
www.konfederacjalewiatan.pl

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m.st. Warszawy w Warszawie
XIII Wydział Gospodarczy KRS