COCIR response to the consultation on the European Commission's proposal for the NIS 2 Directive [1]

COCIR welcomes the opportunity to provide feedback to the European Commission's proposal for a Directive on measures for a high common level of cybersecurity (hereafter the NIS 2 Directive proposal).

COCIR appreciates that the NIS 2 Directive approval builds upon the strengths of the original framework and introduces additional measures to enhance the cybersecurity capacity and capabilities of Member States. Stronger built-in cooperation mechanisms will help improve the EU's resilience and reinforce its regional power.

From a market perspective however, things look quite different as the NIS 2 Directive proposal still leaves several flaws unaddressed, that might perpetuate or aggravate the existing legal fragmentation and overlaps with other regulatory frameworks

The healthcare sector is already heavily regulated, especially when it comes to medical devices and medical software which will in the near future be covered by even more stringent requirements introduced by the Medical Device Regulation.

The digital transformation of health and care has been ramping up in the past years, and certainly under influence of the COVID-19 pandemic crisis, this development has strongly accelerated. The importance and growth of digitalisation in the sector hasn't gone unnoticed and clearly there is a critical need for appropriate cybersecurity and resilience measures.

Cybersecurity in healthcare is however a shared responsibility between industry, healthcare providers, healthcare professionals and other stakeholders. COCIR fully supports and contributes to continuing efforts that raise the level of awareness and security within the sector, recognizing the importance of a secure supply chain.

Having said that, COCIR would like to urge the European Commission to provide the necessary tools, guidance and possible templates – developed in cooperation with stakeholders, including industry – to ensure a smooth and harmonised exchange of information with authorities and within value chains.

In general, COCIR would like to reiterate its call

- To reduce legal fragmentation and create a level playing field
- To provide legal certainty in more clearly articulating the scope, definitions and requirements
- To ensure consistency with existing frameworks and avoid overlaps and administrative burden
- To recognise the value of sector-specific approaches in order to define proportionate and risk-based measures
- To take account of international and European developments in standardisation to define state of the art

- **Scope – Essential entities**

COCIR regrets that the NIS 2 Directive proposal retains the **definition of healthcare providers** from the NIS Directive, ignoring the huge divergence of entities covered in the different Member States, which has led to an **unlevel playing field** for technology suppliers to these entities.

[1] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive

COCIR would like to urge the Commission to **cautiously consider any extension of scope**, in particular if such extension targets specific sectors, like healthcare. Extension should also be based on inherent risks and not necessarily on the intent of malicious actors. Even in the face of increasing threats **proportionality of measures** should prevail.

COCIR is strongly concerned by the fact that the extension of scope is based on **definitions that form part of other newly proposed legislation** which is still subject to a full negotiation and adoption process. This may result in **moving the goalposts** while the NIS 2 Directive proposal is under discussion.

Another worrying aspect is that **rules applicable to entities could become time-critical, and this beyond the control and influence of these entities,** such as in the case where the manufacture of medical devices is considered critical during a public health emergency.

In order to ensure continuity, consistency and legal certainty of the envisioned measures, it is paramount that the scope and definitions used are robust and clear before the legislation comes into force.

- **Scope – Important entities**

COCIR questions the extension of scope that brings in additional entities under the banner of important entities, which are **bound by the same** cybersecurity risk management measures and reporting **obligations as essential entities**.

COCIR is equally concerned by the enlarged scope that **singles out manufacturing facilities** for a selective number of sectors. This also seems to wrongly consider that **supply chain risks** are primarily hardware-related. By not including software suppliers the NIS 2 Directive will fail to properly address security risks in the entire supply chain.

Most entities have no or limited leverage on software suppliers. The burden and responsibility is placed on the users who only have the means to reduce the impact of those security incidents, but are not in a position to control the security of the supplied software. The SolarWinds supply chain attack and the Hafnium exploit of Microsoft Exchange server vulnerabilities are very recent high-profile examples.

In all cases however, any extension of scope should be **risk-based and proportionate**,

- **Scope – Exclusions**

Coherence with other sector-specific frameworks, like for instance the Medical Device Regulation, should be clarified, especially where requirements that could be considered equivalent would lead to an exclusion from the NIS 2 Directive.

It is also unclear from the scope to what extent requirements would **relate to organisations and/or the products and services** they are developing and making available to the market.

- **Minimum harmonisation**

To avoid legal fragmentation Member States should **limit the extent to which they set national requirements** that go beyond the framework and obligations laid down in the NIS 2 Directive proposal.

- **National cybersecurity strategy**

COCIR warmly **welcomes the increased focus on national cybersecurity strategies**, which consider policies (1) to promote and incentivise cybersecurity through **public procurement**; (2) to improve cybersecurity **resilience, skills and awareness**; (3) to better coordinate vulnerability **disclosure and information sharing**.

- **Coordinated vulnerability disclosure and a European vulnerability registry**

COCIR appreciates the more coordinated approach on vulnerability disclosure. With regard to a European vulnerability registry COCIR would like to stress the need for a **careful approach as to how, when and with whom such information would be shared**, and to what extent such information shall be made public.

- **Cybersecurity risk management and reporting**

COCIR would like to underline the need for more **detailed rules on the accountability of management** and on **how to demonstrate compliance with the cybersecurity risk management requirements**, such as and as a minimum (1) risk analysis and information system security policies; (2) incident handling; (3) business continuity and crisis management; (4) supply chain security; (5) security in network and information system acquisition, development and maintenance, including vulnerability handling and disclosure; (6) testing and auditing the effectiveness of cybersecurity risk management measures.

- **Reporting obligations**

COCIR would like to call for more **clarity on the thresholds for reporting** in order to ensure a harmonised approach across Member States.

- **Use of European cybersecurity certification schemes / Standardisation**

COCIR would like to call for a thorough **assessment before introducing any mandatory requirements** of cybersecurity certification. There should be a thoughtful consideration on the **availability and validity of well-recognised international standards** or the voluntary use of cybersecurity certification that can provide an equivalent level of demonstrating compliance.

- **General conditions for imposing administrative fines on essential and important entities**

COCIR would like to emphasise that fines should at all times be **effective, proportionate and dissuasive**. It is also crucial to be transparent on decisive criteria or mitigating factors when setting fines to ensure the threat of maximum fines is not obstructive to organisations intending to **report in good faith** about cybersecurity risks and incidents, especially as they are often an outcome of malicious behaviour of a third party.

COCIR remains fully committed to work with the European Institutions, the Member States and other involved stakeholders in addressing the identified challenges.

COCIR References
COCIR response to the consultation on the NIS Directive Revision (inception impact assessment)
Advancing Cybersecurity of Health and Digital Technologies

About COCIR
COCIR is the European Trade Association representing the medical imaging, radiotherapy, health ICT and electromedical industries.

Founded in 1959, COCIR is a non-profit association headquartered in Brussels (Belgium) with a China Desk based in Beijing since 2007. COCIR is unique as it brings together the healthcare, IT and telecommunications industries. https://www.cocir.org/