

# **COCIR response to the consultation on the Revision of the NIS Directive <sup>1</sup>**

## **(combined roadmap/inception impact assessment)**

COCIR welcomes the opportunity to provide feedback to the combined roadmap and inception impact assessment on the revision of the Directive on Security of Network and Information Systems (NIS Directive) as published by the European Commission.

As we face major technological, cultural and geopolitical shifts in our current society there is a strong need for Europe to reassess its strategic positioning on security-related aspects. Whereas the implementation of the NIS Directive has initially helped to build cybersecurity capacity and capabilities there is a need to anticipate future challenges.

At a more sectoral level this has also been the case for healthcare where the digital transformation and increase in connectivity have drastically changed the threat landscape. This has become even more apparent during the current pandemic crisis where both the heavy pressure and reliance on healthcare services as well as the increase in digital and/or remote health technologies has demonstrated the critical need for cybersecurity and resilience measures.

It is clear from the recently announced EU Security Union Strategy that the NIS Directive will continue to play an instrumental role in building a future-proof security environment.

In order to be well-equipped the revision of the NIS Directive should address following issues

### **1. Identification of Operators of Essential Services**

The European Commission rightly acknowledges that the diverging implementations at national level might hinder a level playing field and exacerbate the risk of cross-border threats.

A revision of the NIS Directive should seek to Increase the level of minimum harmonisation, in particular with regard to the identification of Operators of Essential Services, aligning identification methodologies, criteria and thresholds as much as possible.

### **2. Coordination on cross-border challenges**

The consultation process between Member States on the basis of Article 5(4) should be strengthened. More clarity is needed on how to reach consensus within bilateral or multilateral discussions between Member States.

A more uniform and transparent process should also improve the transparency and certainty for organisations who are active in more than one country.

### **3. Security and incident reporting requirements**

It is not uncommon that equipment which is being used by Operators of Essential Services is already heavily regulated, like in healthcare. This can result in conflicting requirements and unnecessary administrative burden, sometimes further aggravated by legal fragmentation at the national level.

---

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

The European Commission should assess overlaps with other existing regulatory frameworks, such as the General Data Protection Regulation and the Medical Device Regulation. Furthermore, the Commission should actively work with Member States on removing prohibitive rules at the national level.

Technical and organisational measures to manage security risks should not be overly prescriptive, recognise the value of sector-specific approaches and respect international and European standardisation efforts to define state-of-the-art.

A more European and consistent approach to security-related incident reporting should be envisioned in order to avoid duplication and confusion.

#### **4. Structured dialogue at the sectoral level**

COCIR welcomes the creation of a dedicated work stream on health as part of the NIS Cooperation Group's activities, and encourages continued discussions at the sectoral level.

Such structured dialogue should however be expanded to include relevant experts from industry and other stakeholders in order to fully capture the available expertise and knowledge.

COCIR would like to encourage the European Commission to actively follow up on the findings of its report assessing the consistency of the approaches in the identification of operators of essential services.

In order to address the abovementioned challenges COCIR would like to recommend a regulatory intervention introducing targeted changes, that will enable to address some of the existing gaps and inefficiencies, with the aim of creating a more consistent and less fragmented future-proof framework..

Accompanying this, continued efforts are necessary to enhance coordination and consistency mechanisms and to ensure sufficient resources are available at national level to properly enforce compliance with the Directive. Dedicated funding should be made available through the Digital Europe Programme to further support capacity building.

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

#### **COCIR References**

[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. [www.cocir.org](http://www.cocir.org)*