Bld. Brand Whitlock 114 / B-1200 Brussels
T: +32 2 738 78 10

Eoin Kelly
eoin.kelly@applia-europe.eu

APPLiA's Comments on the Proposed Review of the NIS Directive

1. Risk of European Market Fragmentation

APPLiA, representing the home appliance industry in Europe, understands the need for comprehensive rules for a high level of cybersecurity within the European Union. APPLiA's first concern lies in the fact that NIS2 is a Directive rather than a regulation. A regulation would provide the legal certainty needed by manufacturers, whereas a directive fragments the legal landscape and threatens the functioning of the single market. APPLiA's members urge the relevant bodies to reconsider turning NIS2 into a regulation.

2. Scope: Important v Essential Entities

The proposed Directive greatly enlarges the scope. We are of the belief that important entities, including all kinds of manufacturing, might be too large as a scope, and therefore recommend concentrating on critical areas through addressing the essential entities and their respective supply chains.

We would also like to highlight the concern that Article 2 bears the risk of market fragmentation across the European Union, whereby Member States are allowed to decide which entities they put in the scope of the Directive.

3. Software

To appropriately address cybersecurity threats, one should consider the importance of software and its involvement in what becomes the end product. While home appliance manufacturers are included in the scope, software developers have been omitted. Software developers are crucial suppliers and deliver enterprise solutions. As such, we would ask that the scope of affected parties be reconsidered to include software developers. In all cases however, any extension of scope should be risk-based and proportionate.

4. Equal obligations for unequal scenarios

Under the proposed Directive, the obligations for essential and important entities would materially be the same. The conditions for and possible impacts on the operations of essential and important entities are very different. We believe that it is important to highlight the difference between important and essential entities.

For example, important entities should have different treatment to essential entities; we question the logic of having the same reporting obligations for important entities under the current definition (e.g. home appliance manufacturers), as for essential entities like nuclear power stations.

As per Article 18, while the provision of a 24 hour response time for risks/threats to essential entities is understandable, extending the same obligation to manufacturers provides no benefit to society, and puts significant burden on industry, as well as simply not being feasible for many small- and medium-sized enterprises who currently fall under the scope of the Directive.

Article 21 allows Member States to impose rules that require certification of products by the Cybersecurity Act. This could lead to conflicting requirements in different Members States, not only for essential entities. This would fragment the common European market. We urge the Commission to consider this requirement only for critical components, processes and services of essential entities, and also consider alternative approaches to demonstrate compliance with Article 18.

When it comes to important entities, in light of the above issues, we believe the cybersecurity obligations for manufacturers should not be addressed in this Directive but rather in a horizontal NLF product regulation which would put equal obligations on all participants in a given sub-market.

We also wish to highlight our concerns that cybersecurity obligations are increasingly being included in (European) sectoral regulations. It must be prevented that an accumulation of obligations and/or conflicting requirements arise for companies on the basis of the NIS2 and other EU regulations; regulatory overlap should be avoided at all costs.

5. Clarity on when to report

In reference to Article 20.3b, manufacturers need clarity on when to report. We question whether entities have sufficient information to assess the impact on other natural or legal persons as required. Article 20.3b also does not make it clear whether reporting pertains to security issues only within the entity that could impact others, or if this also includes security issues in products and services provided by the entity as part of the reporting obligation, as reporting on security issues in products and services is only mentioned in recital 30 as being on a voluntary basis. Furthermore, we question whether the reporting of "threats" rather than only "incidents" might be excessive, and place undue burden on industry.

The NIS states in Recital 56 that there needs to be a single reporting location for security/privacy. While we understand that the additional voluntary reporting under NIS is the reporting of near-incidents and contributions to the ENISA vulnerability database, we would appreciate clarification on whether there are other reporting obligations for products.

6. Underestimation of costs

We also believe the cost impact estimation is an underestimation. This assessment does not consider some of the other perceived costs to satisfy the supply chain needs, such as:

- Cost for certification of products and services
- Cost to establish, maintain and demonstrate secure development and manufacturing processes
- Certification of organizations/processes
- Cost for the exchange of security information in the supply chain

7. Opportunities: Support the willing

An increasing number of manufacturers from all sectors take the challenges of cybersecurity very seriously. Some of them could benefit (by amendment of the NIS) from financial support for the implementation of sound cybersecurity measures, especially considering SMEs who fall under the current definition of important entities. Particularly in the early stages of securing European networks, it may be difficult to provide products with increased security for competitive market prices. The risk would be that those who take action for more security can suffer significant market share losses. In order to prevent this, a cost sharing fund could incentivize manufacturers and smooth out the transition period.

8. Governance

The governance for multinationals and conglomerates is unclear. As the Directive appears to apply only to European manufacturing locations, we ask for clarification on how the Directive would apply to a company based in the EU, but with a manufacturing plant outside of the EU. We also ask for clarification on how the Directive might impact conglomerate companies, who might for example, manufacture appliances, but also conduct unrelated non-manufacturing activities.

9. Conclusion

We thank the Commission for the opportunity to provide detailed comments on a European framework for cybersecurity. It's clear from the points above that manufacturers require more certainty,

particularly given the significant fines that are being imposed. We greatly look forward to further collaboration with the Commission on these topics.

APPLiA - Home Appliance Europe represents home appliance manufacturers from across Europe. By promoting innovative, sustainable policies and solutions for EU homes, APPLiA has helped build the sector into an economic powerhouse, with an annual turnover of EUR 53 billion, investing over EUR 1.6 billion in R&D activities and creating nearly 1 million jobs.