To the kind attention of **Ditte Juul-Jørgensen**
Director General, DG ENER, European Commission

Towards an effective and implementable network code that meets current and future cybersecurity challenges in the electricity system

Brussels, 8th September 2023

Dear Director General,

With the growth of Decentralised Energy Resources providing flexibility to the increasingly variable energy system, cybersecurity is constantly increasing in relevance. All data-driven business models supporting the clean energy transition should be cybersecure to guarantee both security of supply and consumer engagement based on trust.

smartEn – Smart Energy Europe, the European business organisation integrating the consumer-driven solutions of the clean energy transition, welcomes the Commission's efforts towards a network code on cybersecurity (NCCS) to implement sector-specific cybersecurity rules for the electricity sector.

While we acknowledge that the development of the network code has reached an advanced stage, we nonetheless feel compelled to voice our concerns about critical aspects, notably regarding the scope and objectives, the implementation feasibility and the governance of this network code. More details can be found in the Annex.

We believe that our concerns are of utmost importance and warrant consideration as the code is being finalised and during its subsequent implementation.

We remain at your disposal to ensure the development of an adequate and harmonized level of cybersecurity across the whole electricity system in the EU.

Yours sincerely,

Michael Villa
Executive Director
smartEn

smartEn - Smart Energy Europe
Rue d'Arlon, 63-67
BE-1040 Brussels

info@smarten.eu
www.smarten.eu

ANNEX – Key recommendations for effective and fit-for-purpose cybersecurity network code

Scope and objectives

- Clarify the scope and intended objectives of the NCCS to ensure that it aims to foster a systemic approach to cybersecurity across the entire electricity value chain and support the resilience of the overall service from end to end expected by consumers.
- Strengthen and make as deterministic as possible the classification of entities as high or critical impact entity. It is still unclear which actors will likely be considered as high or critical impact entities and therefore falling under the scope of the NCCS requirements. Considering the significant investments (time, training, costs) to be supported by entities to comply with the NCCS, it is paramount for actors to have as much clarity as possible.

Implementation feasibility

- Ensure that the requirements of the transitional period remain optional at least for the entities that are not grid operators. Given that the applicable requirements of the NCCS are still unknown, it difficult for entities to fully assess the actual feasibility of the new potential obligations and the effort to deliver them. The transitional period should be understood and clarified as a testing period and should serve as a starting point to frame the development of methodologies of the network code, with the involvement of all relevant stakeholders, including market parties.
- Future-proof the NCCS requirements by aligning them with expected regulation and legislation including NIS2 Directive and other legislation expected in the coming 5 to 6 years. This results in a long delay between the end of the risk assessments at the entity level and the effective implementation of the requirements to address those risks identified by entities. In addition, up-to-date additional legislation on cybersecurity are expected to be adopted within that timeframe. It is essential that the NCCS requirements are consistent with other legislation and that they can be readily adapted to future types of cyber-risks.
- Clarify the proposed timelines, sychronisation of processes and deliverables notably for risk assessments, crisis exercises and reports drafting, as major concerns remain regarding the feasibility of the time cycles and scheduling prescribed.

Governance

- Ensure a robust governance framework which currently remains the most critical hurdle for this network code. We have strong concerns over a governance hinged on national competent authorities and with very little or no stakeholders engagement to contribute to the definition of the processes. This creates a risk of lack of consistency and harmonization in the application of cybersecurity requirements among actors across Europe, due to the complexity of the NCCS with many fragmented processes, thus defeating the purpose of a European Network Code.
- Provide EU guidance to the implementation of the code, dealing with all the points raised above, involving all relevant stakeholders through a transparent and inclusive process.

smartEn - Smart Energy Europe
Rue d'Arlon, 63-67
BE-1040 Brussels

info@smarten.eu
www.smarten.eu

ABOUT smartEn - Smart Energy Europe

smartEn is the European business association integrating the consumer-driven solutions of the clean energy transition. We create opportunities for every company, building and car to support an increasingly renewable energy system. Our membership consists of the following companies:

The positions expressed in this document represent the views of smartEn as an association, but not necessarily the opinion of each specific smartEn member.
For further information about smartEn, please visit www.smarten.eu

smartEn - Smart Energy Europe
Rue d'Arlon, 63-67
BE-1040 Brussels

info@smarten.eu
www.smarten.eu