ACER
European Union Agency for the Cooperation of Energy Regulators

Ljubljana, 13 July 2022

ACER-CZ-CGC-sb-2022

acer.igr.dir(2022)5595270

**Ms. Paula Pinho**
Director B Just Transition,
Consumers, Energy Efficiency
and Innovation
Directorate-General for Energy
European Commission
Paula.Pinho(at)ec.europa.eu

***By e-mail only***

**Subject:** **Revision of the Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows**

Dear Ms. Pinho,

Please find enclosed the "Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows" (NCCS) revised by ACER.

On 14 January 2022, ENTSO-E and the EU DSO entity submitted the proposed NCCS to ACER. Pursuant to Article 59(11) of Regulation (EU) 2019/943[1], ACER revised the proposed NCCS to ensure that it complies with the relevant Framework Guideline[2] and contributes to market integration, non-discrimination, effective competition, and the efficient functioning of the market.

In its revision, ACER conducted extensive consultations with the relevant stakeholders and considered the views provided by all involved parties during the drafting of the proposal led by ENTSO-E and the EU DSO entity.

On 13 July 2022, the draft Network Code was given a favourable opinion by the Board of Regulators pursuant to Article 22(5)(a) of Regulation (EU) 2019/942[3].

We would like to highlight two points for your consideration, as they may help improve the legal text during the next phases for the adoption of the delegated act.

[1] Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity OJ L 158 14.6.2019, p. 54
[2] Framework Guideline on sector-specific rules for cybersecurity aspects of cross border electricity flows
[3] Regulation (EU) 2019/942 of the European Parliament and of the Council of 5 June 2019 establishing a European Union Agency for the Cooperation of Energy Regulators OJ L 158 14.6.2019, p. 22

First, we would like to draw your attention on the governance aspects of the NCCS, and in particular, 1) the adoption process of the Terms, Conditions and Methodologies (TCMs) envisaged in Article 8 of the NCCS, and 2) ACER's competences. Regarding the first aspect, we would like to express our serious concerns that the unanimity principle foreseen for the adoption of TCMs will put the effective implementation of this NCCS at significant risk. Based on the existing legislation, we were not able to propose a more robust governance framework, but we would invite the EC to carefully consider this issue. Regarding the second aspect, we would like to emphasise that, during the review process, ACER carefully analysed its role with regard to cybersecurity aspects of cross-border electricity flows. While ACER understands that it has a clear mandate in the process for the establishment of a network code in this regard, ACER's mandate with regard to cybersecurity tasks and vis-à-vis cybersecurity bodies is not entirely evident in the current legislation. For the above reasons, we do see a need to improve the overall governance framework of this NCCS, in particular with regard to the adoption of TCMs, as well as clarify ACER's mandate and competences with regard cybersecurity. In ACER's view, the creation of a clear mandate for ACER on cybersecurity, with the necessary competences and resources, is essential to prevent future uncertainty. For example, ACER could be provided with the competence to issue opinions on cybersecurity aspects of cross-border electricity flows to both NRAs and to the NCCS-NCAs, as this would allow more efficiency in the coordination and cooperation on cybersecurity matters in the electricity sector. Cooperation with ENISA in this regard could also be clarified.

Second, given that the on-going revision of Directive (EU) 2016/1148[4] will be published before the adoption of the NCCS, ACER would like to stress the importance to align the NCCS with the provisions of this revised Directive (NISD2) in order to:

- avoid duplication of supervision regimes and incident reporting channels,
- prevent duplication or fragmentation of tasks for all involved actors,
- align the entry into force of the provisions of the NCCS with those in the NISD2, and
- maintain a coherent approach with the already established cybersecurity governance in the Member States.

ACER has taken the above aspects into consideration in its revision of the NCCS. However, we would find it necessary to further align some provisions once the NISD2 is finalised. For example, it would be essential to align the scope of the NCCS in light of the final NISD2.

We have added further technical considerations in the attached Annexes. In case you have any questions, please do not hesitate to contact Stefano Bracco (Stefano.BRACCO(at)acer.europa.eu) or Manuel Sanchez Jimenez (Manuel.SANCHEZJIMENEZ(at)acer.europa.eu).

[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union OJ L 194, 19.7.2016, p. 1–30

Yours sincerely,

· **SIGNED** –

Christian Zinglersen
Director

Attachments:

- NCCS (as revised by ACER)
- ANNEX I – Proposed Article 11A
- ANNEX II – Considerations regarding Articles 18, 38 and Title VIII of the NCCS

## 1. ANNEX I – PROPOSED ARTICLE 11A

In the last phase of ACER's NCCS review, NRAs discussed the need to share regional costs among Member States and Article 11A (below) was introduced in the text of the NCCS. While the principle was considered to be essential to some NRAs for the correct functioning of the NCCS, there was insufficient time for a detailed analysis on such costs and their distribution. Many NRAs did not support this regional cost sharing concept, for the following reasons:

- the addition of the Article would have implied the development of a specific methodology to ensure its proper implementation, which would have delayed and complicated the NCCS' implementation process;
- while it is difficult to extract cybersecurity costs of information systems ones, it is also not obvious which costs would be distributed at each of the three levels (national, regional and EU, or what would have been excluded because direct consequence of NISD and NISD2);
- the system to be put in place appeared complicated without a demonstration of its workability or added value;
- the article assumed that some costs should be borne by third countries (non-EU Members States), which some Member States view as problematic since the NCCS, as an instrument of EU law, cannot force third countries and their entities to bear costs;
- a linear distribution of costs based on the annual electricity consumption would have assumed that no economy of scale effect was possible, which some Member States considered unrealistic;
- assuming that the costs to be distributed would be mainly a result of investments to reach a certain cybersecurity level and to cover operational costs to maintain this level, the proposed article was considered not to be in line with the principle to incentivise equally all entities to further develop. In fact, this mechanism would have favoured TSOs and DSOs who are not at the expected level yet, who would see contributions to their cybersecurity investments by those TSOs which have already made necessary cybersecurity investments (before the entry into force of the NCCS), resulting in an unequal treatment of all entities.

Therefore, NRAs agreed to remove Article 11A from the NCCS, requesting that ACER flags this topic to the European Commission for consideration and eventually re-introduction, after proper analysis. NRAs would be open to provide further input during the next phase, should this be requested by the Commission.

***(New) Article 11A***

***Cross border cost sharing between TSOs, DSOs in different Member States***

*1. All TSOs and DSOs shall provide a yearly report to the NCCS-NCA and to the NRA in which the costs of the implementation of this Regulation are detailed. This report shall be published by ACER taking due account confidentiality obligations at Article 12.*

*2. The costs referred to in paragraph 1 shall be broken down into:*

*(a) common costs resulting from coordinated activities of all TSOs and DSOs participating in the implementation of this Regulation;*

*(b) regional costs resulting from activities of several but not all TSOs and DSOs cooperating in a certain region;*

*(c) national costs resulting from activities of the TSOs and DSOs in that Member State.*

*The costs referred to in paragraph 2(a) and (b) shall be shared among the Member States and third countries participating in the implementation of this Regulation proportionally to their annual electricity consumption. If there is more than one TSO in a Member State, the Member State shall allocate the costs among the TSOs in that Member State.*

*3. The cost sharing principles shall apply to costs incurred from the entry into force of this Regulation.*

## 2. ANNEX II – CONSIDERATIONS REGARDING ARTICLES 18, 38 AND TITLE VIII OF THE NCCS

### Article 18 - *Cybersecurity risk assessment cycle*

The risk assessment cycle, which is a core part of the overall system, was part of an intense and complex discussion that resulted in the final decision to allow entities in scope to have a 3-year risk assessment cycle instead of a shorter 2-year assessment cycle. Nevertheless, having regard to the urgency to protect energy critical infrastructures under the current socio-political context, ACER would welcome if the European Commission, after the adoption of the NCCS, would encourage entities in those regions that are mature enough, to perform a preliminary risk assessment and to start with risk mitigation steps as soon as possible. The objective would be to complete all the steps and actions in the NCCS without delay, not waiting for the 3-year cycle, especially where the efforts for the entities may take less than a 3-year cycle. This may provide undoubtable benefits for the entire sector and enable a secure further digitalisation of the energy sector, more in line with the current context. This will also have positive effects on trust and confidence of end consumers and energy digitalisation roadmap, which are crucial for the achievement of the decarbonisation targets.

### Article 38 - *Guidance on European cybersecurity certification schemes for ICT products, ICT services and ICT processes*

The solution offered in the NCCS to mitigate the risks linked to the supply chain introduces a first step forward in addressing supply chain risks linked to cybersecurity in the energy sector, to be in place until the implementation of the Title III of the Regulation (EU) 2019/881[5] (Cybersecurity Act) would allow the use of more suitable means. Having this in mind, some of the institutional stakeholders and ACER are of the opinion that all provisions that would derive from the implementation of the Cybersecurity Act, when schemes are available, will provide the best solution to existing supply chain issues, therefore the NCCS should be re-considered for a review once suitable certification schemes for energy under the Cybersecurity Act will be available at a later stage. This will enable a general homogenisation of the landscape and the use of proper tools by entities in scope.

### TITLE VIII - *ESSENTIAL INFORMATION FLOWS, CYBERSECURITY INCIDENT AND CRISIS MANAGEMENT*

The crisis management provisions of the NCCS can be further aligned with the provisions in the NISD2 and in particular establishing communication flows to cross-cut and support the “The European cyber crises liaison organisation network (EU - CyCLONe)”, with the role to

[5] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJ L 151, 7.6.2019, p. 15–69

support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of relevant information among Member States and Union institutions, bodies and agencies. As the NCCS also includes elements to address crisis management in the event of cyber incidents with an impact on the electricity grid, it would be advisable to introduce provisions in the NCCS for the establishment of information flows to/from EU – CyCLONe network in events such as the preparation of plans to respond to such crisis or critical cybersecurity incidents affecting the electricity sector and beyond. This would provide coherence in the way crises linked to cybersecurity incidents with high impact will be coordinated at EU level based also on plans, also with the help and cooperation of all necessary stakeholders. Such provisions for the establishment of information flows to/from EU – CyCLONe network were already requested by some of the stakeholders, however their introduction in the NCCS was not possible prior to the formal adoption of the NISD2.