– Consultation response –

Joint-feedback on draft Commission Delegated Regulation establishing a Network Code for Cybersecurity Aspects of Cross-Border Electricity Flows

Brussels, 17 November 2023 | **Europex and the All NEMO Committee welcome the opportunity to respond to the Commission consultation on the draft Commission Delegated Regulation establishing a Network Code for Cybersecurity Aspects of Cross-Border Electricity Flows (NC CS). While we generally support the initiative to enhance cybersecurity in the energy system, as far as the current draft is concerned, we call for crucial improvements in relation to stakeholder involvement, planning certainty, alignment with other legislative acts and existing international standards, as well as proper safeguards for sensitive information and more inclusive provisions on cost recovery.**

Europex' membership includes Nominated Electricity Market Operators (NEMOs) as well as Organised Marketplaces (OMPs), which both fall within the scope of the draft NC CS provided that they are identified as high-impact or critical-impact entities. Europex has previously contributed to related consultations (jointly with the All NEMO Committee[1] and separately[2]) and also issued an opinion statement[3].

While the draft Commission Delegation Regulation (CDR) clarifies several key concepts and requirements, we still see room for significant improvement and would like to make the following recommendations:

1) Improve stakeholder involvement to increase framework robustness

NEMOs and OMPs are vital actors in enabling cross-border electricity flows. Therefore, they should also be included in the conception and implementation of the related cybersecurity framework. In comparison to previous drafts and discussions, the current text, however, limits the involvement of NEMOs and OMPs in this respect. This sudden change should be undone and the possibility for NEMOs and OMPs to contribute to the drafting of methodologies should be reinstated. Excluding

[1] *Europex / All NEMO Committee*, ACER Consultation on the Draft Framework Guideline on sector- specific rules for cybersecurity aspects of cross-border electricity flows, 29/06/2021. Available at: https://www.europex.org/consultation-responses/fg-cybersecurity/

[2] *Europex*, ENTSO-E Consultation on the Network Code for Cybersecurity Aspects of Cross-Border Electricity Flows, 10/12/2021. Available at: https://www.europex.org/consultation-responses/entso-e-consultation-on-the-network-code-for-cybersecurity-aspects-of-cross-border-electricity-flows/

[3] *Europex*, Opinion statement on draft Network Code for Cybersecurity Aspects of Cross-border Electricity Flows, 07/03/2022. Available at: https://www.europex.org/position-papers/europex-comments-on-draft-network-code-for-cybersecurity-aspects-of-cross-border-electricity-flows/

NEMOs and OMPs from the drafting process would jeopardise the robustness of the overall framework.

To ensure efficient stakeholder involvement, we call for an extension of the minimum consultation period in Article 9(1) from one to two months and for adding greater detail to the modalities and frequency of stakeholder involvement in Article 10.

2) Closely align with international standards

The cybersecurity risk assessment methodologies which are to be developed by the TSOs pursuant to Article 17 are crucial for the NC CS in general and for defining the Electricity Cybersecurity Impact Index (ECII) values in particular. Against this background, it is regrettable that there is so far no further guidance on the content of the methodologies and that stakeholder involvement remains limited. Hence, the final NC CS should include clear requirements for TSOs to follow established international standards when defining methodologies and performing risk assessments. In addition, NEMOs and OMPs should be involved in developing the methodologies. Such specifications would alleviate the risk of entities having to apply different cybersecurity standards.

3) Reduce uncertainty over scope

In terms of legal certainty and planning security, the lack of clarity over when an entity will be classified as high-impact or critical-impact in accordance with Article 23 remains unsatisfactory. As it stands, entities may have to wait up to 48 months after the entry into force of the NC CS to have certainty over whether they are considered to fall within its scope or not (see Article 23(6)). Considering that compliance with the NC CS will in some cases necessitate important investments and the mobilisation of resources, the identification of high-impact or critical-impact entities should be streamlined and made more transparent, while guaranteeing swift legal remedy.

4) Avoid regulatory patchwork

The possibility for competent authorities to delegate tasks pursuant to Article 4(3) creates additional uncertainty for entities in scope of the NC CS. On a similar note, it is unclear why the benchmarking analysis under Article 13(2) is to be carried out by NRAs instead of the competent authorities for cybersecurity. To ensure the overall efficiency of the cybersecurity framework, an unnecessarily complex regulatory patchwork must be avoided.

5) Minimise regulatory overlap

NEMOs and OMPs are already fulfilling high cybersecurity standards and are typically subject to the Digital Operational Resilience Act (DORA)[4] and obligations under the Network and Information

[4] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

Security (NIS 2) Directive[5]. As the future NC CS would be sector-specific legislation, it is crucial to avoid conflicting rules and inconsistencies between the NC CS and NIS 2. Hence, we suggest including a clause analogous to Article 1(2) of DORA.[6]

Considering that several NEMOs and OMPs operate in more than one Member State, there is great concern that situations may arise where entities within scope of the NC CS would face parallel reporting obligations in each of the Member States they operate in, thus incurring a disproportionate financial and administrative burden. Different competent authorities may have different approaches to cybersecurity. Therefore, any divergence in interpretation or a diverging application should be avoided and obligations be streamlined. The future NC CS should be complemented by a clause stating that the identification of an entity as high-impact or critical-impact as well as any ensuing supervisory or enforcement measures shall only be taken by the competent authority of the Member State in which the entity is legally established. Such a clarification would be particularly pertinent in the case of NEMOs, who – while bearing the same responsibility for Single Day Ahead Coupling (SDAC) and Single Intraday Coupling (SIDC) – may be assessed differently in different Member States. Situations might therefore arise, where the same NEMO is considered a high-impact entity in one Member State and a critical-impact entity in another.

6) Ensure confidentiality to minimise transparency abuse

Article 22(4) requires the release of a public version of the comprehensive cross-border electricity cybersecurity risk assessment report. While transparency is a laudable objective, publishing information on cybersecurity setups of high-impact and critical-impact entities constitutes an unacceptable risk. In the absence of proper safeguards, the comprehensive cross-border electricity cybersecurity risk assessment report should not be made public and only be shared in a restricted environment.

7) Enable cost recovery for all high-impact and critical-impact entities

The provisions in Article 11 of the draft NC CS on cost recovery are only applicable to TSOs and DSOs. Similar support for cost recovery should be available for all high-impact and critical-impact entities, including NEMOs and OMPs, as this would incentivise cybersecurity investments.

[5] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148

[6] Article 1(2) of Regulation (EU) 2022/2554 reads: „In relation to financial entities identified as essential or important entities pursuant to national rules transposing Article 3 of Directive (EU) 2022/2555, this Regulation shall be considered a sector-specific Union legal act for the purposes of Article 4 of that Directive."

About Europex

Europex is a not-for-profit association of European energy exchanges with 34 members. It represents the interests of exchange-based wholesale electricity, gas and environmental markets, focuses on developments of the European regulatory framework for wholesale energy trading and provides a discussion platform at European level.

Contact

Europex – Association of European Energy Exchanges
Rue Archimède 44
1000 Brussels, Belgium

Phone: +32 2 512 34 10
Website: www.europex.org
Email: secretariat@europex.org
X: @Europex_energy

EU Transparency Register: 50679663522-75

About the All NEMO Committee

The All NEMO Committee facilitates the cooperation among NEMOs for all common European tasks necessary for the efficient and secure design, implementation and operation of single day-ahead and intraday coupling. The All NEMO Committee is a contractual decision making body without legal personality, formed by the appointed representatives of each NEMO.

For more information: www.nemo-committee.eu