EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR ENERGY

Directorate B - Just Transition, Consumers, Energy Efficiency and Innovation
The Acting Director

Brussels
ENER.B.4/MK/gt s(2021)585504

ACER
Christian Zinglersen
Director
Trg republike 3
1000 Ljubljana
Slovenia

Subject: **Invitation to draft framework guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows**

Dear Mr Zinglersen,

The Electricity Market Regulation[1] (hereinafter called 'Regulation') lays down provisions for establishing a network code for enhancing the cybersecurity of cross-border electricity flows. Article 59, paragraph 2 of the Regulation empowers the Commission to adopt delegated acts, supplementing the provisions of the Regulation in accordance with Article 68, concerning the establishment of network codes in a number of areas. With regard to cybersecurity, Article 59, paragraph 2(e) foresees sector-specific rules for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management.

Furthermore, Commission Implementing Decision (EU) 2020/1479[2] establishes a priority list for the development of network codes and guidelines for electricity for the period from 2020 to 2023. Article 1 of this Decision provides for the development of sector-specific rules for cybersecurity aspects of cross-border electricity flow, including rules on common minimum requirements, planning, monitoring, reporting and crisis management.

The network code should be developed without prejudice to the provisions of the Risk Preparedness Regulation[3] and should take into account any existing methodologies that include cyber-related aspects.[4]

[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] Commission Implementing Decision (EU) 2020/1479 of 14 October 2020 establishing priority lists for the development of network codes and guidelines for electricity for the period from 2020 to 2023 and for gas in 2020

[3] Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, OJ L 158, 14.6.2019, p. 1

Commission européenne/Europese Commissie, 1049 Bruxelles/Brussel, BELGIQUE/BELGIË - Tel. +32 22991111
Office: DM24 04/059 - Tel. direct line +32 22953798
Hans.Van-Steen@ec.europa.eu

The COVID crisis has accelerated the dependency on digitalisation, including in the energy sector. The Commission has explained in its communications on the Energy Sector Integration[5], the Security Union Strategy[6] and the Cybersecurity Strategy[7] that the reinforcement of cybersecurity in the electricity sector was needed in view of the rapidly evolving threats landscape and at the same time the rapid transformation of the electricity sector in the clean energy transition. The communications stress the importance of drafting the network code on cybersecurity of the cross-border electricity flows by the end of 2021 in view of an adoption by the Commission in 2022.

I therefore invite ACER to assume the role assigned to the Agency under Article 59 of the Regulation and submit to the Commission a non-binding framework guideline for the development of the network code on the cybersecurity of cross-border electricity flows.

The Commission should request ACER to submit framework guidelines within a reasonable period not exceeding six months. However, in the COVID circumstances the need to address the cybersecurity aspects of cross-border electricity flows is a matter of urgency. ACER has already been involved in the informal drafting which has been taking place since February 2020, and the relevant stakeholders have already been consulted on the principle and then on the informal interim report of the network code. In these circumstances, in the case of the framework guideline for this specific network code, a shorter period than the maximum period mentioned above seems justified and reasonable and should be aimed at. I would therefore like to invite ACER to do its best to provide the framework guideline as soon as possible, and in any event without using the full six months period referred to in the Regulation.

In accordance with the Regulation, the framework guideline should describe principles which 1) are clear and objective for the development of the network code and which 2) contribute to market integration, non-discrimination, effective competition, and the efficient functioning of the market.

Furthermore, the framework guideline should take into account the following principles as defined during the preparatory work in which ACER participated:

- How to protect the energy systems based on current and future threats and risks.
- How to support the functioning of the European society and economy in crisis situation.
- How to create trust and transparency for cybersecurity in the supply chain for components and vendors used in the energy sector.
- How to harmonise maturity and resilience for cybersecurity across EU with defined minimum level while favouring higher maturity.

In particular, the framework guidelines should address the following conditions, which shall be addressed by the network code:

---

[4] The Risk Preparedness Regulation ensures that cyber-incidents are properly identified as a risk, and that the measures taken to address them are properly reflected in the risk-preparedness plans.

- Clearly define the scope of the network code, as well as the entities being subject to the network code;
- Establish a sound governance for the overall process of ensuring the cybersecurity of cross-border electricity flows (both from a strategic & planning and operational perspective, and including responsibilities related to monitoring, reporting and crisis management). Clear roles shall be defined for ENTSO-EU, the future EU-DSO Entity, the Member States authorities, European Commission, ACER, ENISA and the entities subject to the provisions of the network code;
- Carry out cross-border cybersecurity risk assessments;
- Establish rules for effectively managing and mitigating the identified cross-border risks, based on a uniform approach (e.g. adoption of Information Security Management Systems ISO/IEC 27001);
- Adopt minimum cybersecurity controls and requirements;
- Address the risks originating from 1) the supply chains and 2) legacy technologies;
- Provide a framework for effectively and timely sharing of technical information regarding: cyber-attacks, cyber threats and near misses, early warnings, other information relevant for preventing, detecting, responding to or mitigating cybersecurity incidents;
- Provide the possibility to measure the actual status of the implementation of cybersecurity measures against an energy cybersecurity maturity framework.

The guidelines could also:

- Provide the possibility for additional guidance on complementary topics such as crisis management and supply chain security;
- Cover additional aspects conducive to enhanced cyber resilience, including: arrangements for carrying out joint exercises, peer reviews, inspections and coordinated inspections in the event of an incident, other means of enhanced cooperation on cybersecurity.

The framework guideline should take into account the Commission Recommendation on cybersecurity in the energy sector[8] and address the specificities of the energy sector such as:

- Real-time requirements of energy infrastructure components;
- Cascading effects;
- Legacy and state-of-the-art technology.

The framework guidelines should take into account the considerable preparatory work completed so far, which consists of the recommendations of the Smart Grid Task Force Expert Group 2 report[9] and the recommendations of the ENTSO-E/ DSO associations informal interim report[10].

The framework guideline should take into account the Commission proposal for a Directive on measures for common high level of cybersecurity across the Union (revised

[8] Commission Recommendation (EU) 2019/553 of 3 April 2019 on cybersecurity in the energy sector

[9] https://ec.europa.eu/energy/sites/ener/files/sgtf_eg2_report_final_report_2019.pdf

[10] Second interim report of 31 October 2020, Recommendations for the European Commission

on a Network Code on Cybersecurity, please find enclosed

NIS Directive or 'NIS 2')[11], and the Commission proposal on a new Directive on the resilience of critical entities[12], bearing in mind that the proposals are not adopted yet.

For the sake of an efficient and transparent process, I have no objections to this letter being shared with all relevant stakeholders.

Yours sincerely,

Hans van Steen

Enclosure: Second interim report "Recommendations for the European Commission on a Network Code on Cybersecurity", by the informal drafting team (ENTSO-E/DSOs)

c.c.: Sonya Twohig, ENTSO-E
Carmen Gimeno, GEODE
Kristian Ruby, Eurelectric
Gert De Block, CEDEC
Roberto Zangrandi, EDSO for smart grid

[11] COM(2020) 823 final

[12] COM(2020) 829 final