– Consultation response –

ACER Consultation on the Draft Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows

Brussels, 29 June 2021 | We welcome this opportunity to provide input on ACER's draft Framework Guideline on electricity sector-specific rules for cybersecurity and see the value in ensuring a high standard of cybersecurity. However, in this response we would like to stress that the FG should complement existing cybersecurity requirements such as those in the proposed NIS 2 Directive and avoid unnecessary duplication. Furthermore, harmonisation across Member States will be critical to identify cross-border cybersecurity risks efficiently and ensure that communication obligations are well tailored as to avoid unduly increasing the workload of entities in scope.

Please find below selected responses to the consultation questionnaire.

Does the Framework Guideline contribute to the following objectives?

To further protect cross-border electricity flows, in particular critical processes, assets and operations from current and future cyber threats?	Yes	**No**
To promote a culture that aims to continuously improve the cybersecurity maturity and not to simply comply with the minimum level	**Yes**	No
To mitigate the impact of cyber incidents or attacks or to promote preparedness and resilience in case of cyber incidents or attacks?	Yes	**No**
To support the functioning of the European society and economy in a crisis situation caused by a cyber-incident or attack, with the potential of cascading effects?	Yes	**No**
To create and promote trust, transparency and coordination in the supply chain of systems and services used in the critical operations, processes and functions of the electricity sector?	Yes	**No**

Although the Framework Guideline (FG) might have a more specific objective, we fail to see the value added by the proposed requirements to the existing regulatory frameworks of the NIS Directive and its implementation acts as well as the proposed NIS2 Directive. We therefore believe a stock-taking exercise of the latter is very much needed to ensure the FG is complementing rather than duplicating. If not, duplicative regulatory requirements will take away resources needed to deal with possible threats.

Do you see any gaps concerning the cybersecurity of cross-border electricity flows which the draft FG proposal should address?

Yes, at this stage we are very concerned about a duplication of requirements (see Q1). However, we would also like to raise the importance of ensuring a certain level of secrecy of information. The final network code should, for example, refrain from publishing lists of essential and important services mentioned under point 1.5 of the FG. Published databases, registries and similar documents can pose a risk to the overall security, as attackers would be able to easily detect weak links.

Does the FG applicability cover all entities that may have an impact on cross-border electricity flows, as a consequence of a cybersecurity incident/attack?

We recommend limiting the applicability for NEMOs to where it directly concerns cross-border electricity flows. It is our understanding that trading venues & clearing houses are not defined as essential service providers (please note these entities have extensive coverage via financial regulatory oversight).

To avoid substantial overlap with the upcoming NIS 2 Directive we believe the FG should either

a) Exclude entities which will be covered by NIS 2, or
b) Allow for a partial overlap regarding entities covered, but not duplicating requirements covered by existing frameworks (less preferable)

The proposed FG prescribes a process to differentiate electricity undertakings based on their level of criticality/risk, and setting different obligations depending on their criticality/risk level. Do you think that the proposed transition is the most appropriate?

No, we believe a transitional phase is not needed as the NIS2 Directive will soon be implemented. A transition assessment by the institutions named under 1.6 of the FG bears a risk of arbitrariness as the methodology is not comprehensively developed. As a result, entities might be considered essential within this transition period and incur unnecessary costs to comply, but ultimately be deemed non-essential in the established methodology. As the adoption of such FG takes time - for both law maker and law subject – sufficient time should be given for the transition.

The FG proposes that all small and micro-businesses, with the exception of those that, despite their size, are defined as important/essential electricity undertakings, shall be exempted from the obligations set in the NC. Do you think this approach is consistent with the general idea to uplift and harmonise the cybersecurity level?

While we agree in principle with this approach, we find that additional clarity is needed on when a small or micro-business will be defined as important/essential and which authority will be responsible for this definition.

Do you find that the proposed FG succeeds in establishing a sound governance for the overall process of ensuring the cybersecurity of cross-border electricity flows?

Yes, we support the lean governance structure proposed. It is essential to ensure that existing agencies with competences on Information Security agree on cooperation & on a single energy specific contact point for energy specific incidents (SPOC), which is to be informed in case of a CS incident. We support the idea, as under current regulation, power exchanges are often already required to report to multiple institutions with differing standards. There is significant potential to reduce efforts to report and self-assess. In particular, a SPOC could reduce these efforts & avoid double-reporting.

Is the decision on setting up the conditions assigned to the right decision group or should that decision be taken at a higher strategic level in respect to what is proposed in the draft, having in mind that this decision will be extremely sensitive?

Rather than setting up a new process to determine the conditions to classify and distinguish entities, we believe existing lists can be used, such as those under NIS2 and relevant national legislation (BSI-KritisV for example). Not having a consistent and clear definition of essential and important electricity undertakings could lead to unnecessary complexity.

The draft FG proposes a high-level methodology for cross border risk assessment presented in chapter 3 and based on three consecutive levels. Is this high-level methodology adequate for assessing and managing risks of cross-border electricity flows?

Identification scenarios having the potential to escalate should be identified commonly. To ensure harmonisation and efficiency, Member States should not decide on relevant scenarios themselves. Rather, a newly established European CERT could take the function of commonly identifying and defining relevant scenarios. This proposal is based on the Computer Incident Response Centre Luxembourg which is a government-driven initiative designed to gather, review, report and respond to Cyber Security threats and incidents.

Are the 'minimum' and 'advanced' cybersecurity requirements applied to the right entities?

They are applied to the right entities, but they are not proportional, and they partially fit with the purpose to protect cross-border electricity flows from cybersecurity threats. It is difficult to respond to the question as essential and important entities are not clearly defined under the NC. As mentioned under question 4, a burden of duplication should be prevented. Only a harmonised and efficient cross-sectoral regime will allow for optimal strengthening and usage of existing and future Cyber Security (CS) capacities.

How should a common cybersecurity framework protecting cross-border electricity flows be established and enforced?

A combination of the suggestions the ensures common minimum requirements are met is most desirable. There should be the possibility that these minimum requirements can be met through different approaches. For example, entities already certified under a certain standard should be able to make use of their certification while other entities will have the possibility to meet the requirements through other measures proposed.

The proposed FG extends the obligation of the cybersecurity measures and standards to "essential service suppliers" to which an entity may outsource essential services, operations of essential assets and services, or a full essential process, that has an impact on the cybersecurity of cross-border electricity flows. Do you think this approach is correct?

Yes, it is crucial that the same standards and obligations are applied along the entire supply chain toavoid the any "weakest link" poses a risk to the system and ensure a common level of cybersecurity. We support basing the decision on a risk-based approach.

The FG proposes the use of designated Electricity Undertaking Security Operation Centre (SOC) capabilities to enable information sharing and to smooth incident response flows from all electricity undertakings. Do you agree with this approach?

The proposed approach is feasible and therefore needs to be reviewed. CSIRTs are best placed to enable information sharing and incident response, as such we support an approach in which European CSIRTs are strengthened and provided with sufficient resources to enable them to take on these additional responsibilities. This is particularly important as Cyber Security is a cross-sectoral issue that cannot be treated only sector specifically.

The draft FG proposes the adoption of SOC to overcome other needs that go beyond the simple information sharing. Do you think that this secondary role is appropriate for the SOC?

No, the secondary role of SOCs may unnecessarily increase the points of contact needed for information sharing and lead to repetition of reporting.

Do you believe a Cybersecurity Electricity Early Warning System as described in the proposed FG chapter 5.4 is necessary?

Yes, we support the proposal that the Electricity Cybersecurity Early Warning System (ECEWS) should be covered by ENISA and CERT-EU.

Concerning the obligation for essential electricity undertakings to take part in cybersecurity exercise as described in chapter 6 of the draft FG, please select one of the following options.'

This is in line with the objectives, and it contributes to the substantial improvement of the cybersecurity posture necessary for cross-border electricity flows. We fully support the

proposal that essential electricity undertakings take part in cybersecurity exercises to detect issues and share best practices. These exercises should be conducted in close cooperation with existing authorities such as the national CSIRTs.

The proposed FG suggest monitoring obligations to verify the effectiveness in the implementation of the NC. In this respect, do you think they are appropriate?

The proposed monitoring obligations are excessive, and a major revision of the principles is suggested. A gap-analysis should be conducted before additional monitoring, benchmarking, and reporting obligations are put in place. It is necessary to look closely at the existing obligations of entities to ensure efficiency (both in terms of monetary cost and time) and avoid unnecessary duplications.

The proposed FG suggests benchmarking obligations to control the efficiency and prudence in cybersecurity expenditure, resulting from the implementation of the NC. Do you think that the benchmarking obligations are appropriate?

We welcome appropriate benchmarking obligations; however, benchmarking must not focus solely on the cybersecurity expenditure but also consider the overall maturity of cybersecurity measures in place. Furthermore, benchmarking obligations in the NC should not duplicate existing obligations or require excessive additional effort without justification.

The proposed FG suggests reporting obligations: the aim of the reporting obligations is to facilitate informed high-level decisions on the revision of the network code.

As proposed above, a gap-analysis should be conducted, and potential reporting obligations should carefully be evaluated to ensure efficiency and prevent unnecessary duplications.

Do you think the proposed FG sufficiently cover cybersecurity aspects of:

a) Real-time requirements of energy infrastructure components?
   a) Fairly covered

b) Risk of cascading effects?
   a) Fairly covered

c) Mix of legacy and state-of-the-art technology?
   a) Fairly covered

Additional comments

We would like to underscore that the FG should be based on established international standards for managing cybersecurity - namely NIST (National Institute for Standards and Technology) and the Cybersecurity Framework (CSF), and not only rely on the ISO/IEC 2700X standards referenced in the current proposed FG. Recently the aforementioned standards have been used as a basis for guidance on cyber resilience, such as CPMI-IOSCO Guidance on cyber resilience for financial market infrastructure and G7 Fundamental Elements of Cybersecurity for the Financial Sector.

As a more general comment, we would also like to highlight that additional stakeholder engagement would be greatly appreciated as this process continues.

About

Europex is a not-for-profit association of European energy exchanges with 29 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
Address: Rue Archimède 44, 1000 Brussels, Belgium
Phone: +32 2 512 34 10
Website: www.europex.org
Email: secretariat@europex.org
Twitter: @Europex_energy