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

Fields marked with * are mandatory.

General introduction

The purpose of the non-binding Framework Guideline (FG) is to set high-level principles that should be further elaborated in the Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows.

The role of the FG and of the following network code, is to supplement and further specialise existing cybersecurity and risk preparedness directives and regulations, introducing viable solutions to identified cybersecurity gaps and risks.

The objective of the network code, based on the draft FG principle, should be to solve, mitigate and prevent the potential high impact or materialization of cybersecurity risks, as well as to prevent those cybersecurity attacks or incidents that may impact real time operations (causing cascade effects).

ACER invites all concerned stakeholders to contribute to the public consultation, and therefore to define and shape the final Framework Guideline.

Next steps:

- ACER will analyse the responses received in July 2021 and will deliver a final version of the FG to the European Commission.
- In July 2021, ACER will publish a summary of the consultation, including an evaluation of the responses.
- ACER will publish all responses received and the identity of their respective stakeholders (unless stated otherwise). For this reason, please indicate if your response may be publicly disclosed or not, and if you agree with the data protection policy.

All concerned stakeholders are invited to respond to the public consultation on the proposed Framework Guideline.

The public consultation will run between 30 April 2021 to 29 June 2021 at 23:59 Ljubljana Time.

ACER will only accept responses in electronic format, no other format will be accepted. **In case of technical problems with the submission of your responses please contact DFG-NC-CS@acer.europa.eu.**

ACER will organise a workshop to introduce and explain the content of the proposed Framework Guideline, in May 2021. More information will be circulated via ACER Infoflash closer to the date of the event.

* First Name

[redacted]

* Last Name

[redacted]

* Company/Institution

Energy Community Secretariat

* Type of business

International Organization

Address

Am Hof 4 Level 5, 1010 Vienna, Austria

* Contact email

[redacted]

Phone

[redacted]

Country

AT - Austria

I confirm that I have read the data protection notice in this link and accepted.

- (•) Yes
- ( ) No

I authorise the disclosure of my identity together with my response

- (•) Yes
- ( ) No (I want my response being completely anonymous)

1. Meeting the general objectives

Question 1 - Does the Framework Guideline contribute to the following objectives?

	Yes	No
To further protect cross-border electricity flows, in particular critical processes, assets and operations from current and future cyber threats?	(•)	( )

To promote a culture that aims to continuously improve the cybersecurity maturity and not to simply comply with the minimum level	◉	○
To mitigate the impact of cyber incidents or attacks or to promote preparedness and resilience in case of cyber incidents or attacks?	◉	○
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?	◉	○
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?	◉	○

Please, provide a short explanation justifying your assessment, if needed:

600 character(s) maximum

The Guidelines seam to provide a detailed and well-defined platform for establishment of harmonized rules and criteria in the cybersecurity environment specific to the needs for protection of cross-border electricity flows and resilience of the related EU entities. In many ways, it makes the task of ENTSO-E straightforward and focused.
After the basic recommend provided by DG ENER in 2019, energy-specific aspects of cybersecurity have not gained the required attention to cope with the growing threats - the Network Code (based on the Guidelines) will fill a large (and growing) necessity.

Question 2 - Do you see any gaps concerning the cybersecurity of cross-border electricity flows which the draft FG proposal should address?

- ◉ Yes
- ○ No

If yes, provide details

600 character(s) maximum

No document is perfect.
Among other minor flows, main shortcoming is the void in references related to non-EU aspects of cybersecurity that should be taken into consideration in the widely interconnected and rapidly integrating environment of cross-border electricity exchanges.
Most relevant is the missing mechanisms for alleviation of cybersecurity threats exchanged (in both directions) with the neighboring Energy Community Contracting Parties. The Item 1.4 provides only the administrative context with no policy analysis or applicable proposals, useful mostly for remote environments.

2. Scope, applicability and exemptions.

Question 3 - The draft FG suggests that the Network Code shall apply to public and private electricity undertakings including suppliers, DSOs, TSOs, producers, nominated electricity market operators, electricity market participants (aggregators, demand response and energy storage services), ENTSO-E, EU-DSO, ACER, Regional Coordination Centres and essential service suppliers (as defined in the FG). 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?

- ○ Yes
- ◉ No

Please, explain who is missing and why

600 character(s) maximum

As mentioned before, the "administrative" scope is better completed than the geographical scope - which should distinguish in treatment of (all categories of) stakeholders in the Energy Community (and eventually other relevant neighboring countries) and the undertakings participating in the energy flows which are (simply) represented.
Additionally, the small and micro entities (in the Energy Community) may participate in the supply chain, and deserve attention and policy considerations (please refer to the comments on the treatment of SME in the FG).

3. Classifications of applicable entities and transitional measures

Question 4 - 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. This will imply a transition period until the full system is established and will require the establishment of a proper governance to duly manage the entire risk assessment process. Do you think that the proposed transition is the most appropriate?

- ○ Yes
- ◉ No

Would you suggest another transition approach and why?

600 character(s) maximum

Notwithstanding the timing assessment, the criticality/risk assessment paradigm should include the category of risk stemming from the interconnection with non-EU neighboring countries (in particular the Energy |Community). The threats may come from spill-over in the digital domain and/or cascading effects in the energy domain.
That would provide basis to extend the policy considerations and define mechanisms to:
- protect EU Member States from such threats, and
- provide cooperation and support mechanisms to alleviating cybersecurity risk (stemming from the EU) in these countries.

Question 5 – 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 (excluding the general requirements for cyber hygiene). Do you think this approach is consistent with the general idea to uplift and harmonise the cybersecurity level within the ecosystem in order to efficiently protect cross-border electricity flows?

- ○ Yes
- ◉ No

Please, explain why:

600 character(s) maximum

The SMEs have no capacity to set the same environment as large undertakings and they must be treated separately. However, they are interconnected and the digital layer is equally exposed to threats. In addition, they are increasingly commercialized, which extends the scope of threats and expands the attack surface. SME should not be omitted. FG (and NC) should include a set of mechanism dedicated to ALL SMEs which in overall should provide corresponding level of risk that is acceptable for the large entities. The extensive SME / prosumer costs in this context may eventually be socialized.

4. Cybersecurity security governance

Question 6 - 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
- ◉ No

What is missing and where do you think ACER should put more attention to?

600 character(s) maximum

In general the governance context is well defined, comprehensive, and seemingly functional. It is, however at odds with the draft NIS 2 Directive in certain aspects (even looks more related to the old NIS Directive). For example, the use of "essential" and "important" entities is based on the level of risk (logical) - however in the Directive it is based in the sectors of the economy. There are also mechanisms in the NIS 2 that are not mentioned here.
It is important to harmonize the acts as much as possible and avoid possible misconception.

Question 7 – The proposed FG describes the process and governance to determine the conditions to classify and distinguish electricity undertakings with different risk profiles for cross-border electricity flows. 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?

- ◉ Yes, the decision is taken by the right decision group.
- ○ No, the decision shall be taken at a higher strategic level.

Please, explain shortly by whom and your reasoning:

600 character(s) maximum

The distinction refers to a scope of mandatory measures / obligations (and incurred costs) to be attributed (or not) to a set of entities - determined as essential or important.
It should be mentioned that NIS 2 Directive considered ALL medium and large entities (operating in the particular sector) as "essential" - it is the Resilience Directive which imposes the selection and registration of particular "critical" (or "equivalent") entities.
The approach in the FG may have advantages in the enforcement. It should be flexible enough.

Question 8 – Please, tell us which aspects of the proposed governance may better be developed further.
Per each line covering the governance aspects of each chapter, please select all statements that can fit.

	Roles are defined	Responsibilities are assigned	Authorities are defined	Accountability is clear	High level decisional processes are defined
General Governance	☑	☑	☐	☑	☐
Cross Border Risk Management	☐	☑	☑	☐	☐
Common Electricity Cybersecurity Level	☑	☐	☑	☐	☑
Essential information flows, Incident and Crisis Management	☑	☑	☑	☑	☑
Other aspects	☑	☐	☐	☑	☐

Please, add comments in case you may suggest changes to the attribution of roles, responsibilities, authorities, and to the envisaged processes, where described.

600 character(s) maximum

In some aspects the overall administrative structure appears complex and rigid, in particular in the context of data "sanitation" models. The role and the direct participation of the primary stakeholders should be enhanced - assuming that they are interested to take the responsibility (which should be in their interest). Their direct cooperation should be simplified and enhanced (at least in some cases, and as an option). That may provide for higher efficiency.

5. Cross border risk management

Question 9 – 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?

- ○ Yes
- ◉ No

Would you suggest any alternative way to proceed?

600 character(s) maximum

It is actually adequate, except in the context of the EU perimeter borders. As mentioned before, the neighboring Energy Community Contracting Parties should be included in the cross-border risk assessment exercises - which includes a cooperation mechanism on technical level and a policy mechanism (instrument of cooperation). This will contribute for more comprehensive risk assessment.
- it is important to notice that the Energy Community is heading in 2021 to adopt the Clean Energy Package as its mandatory acquis which will provide the required legal background for enforcement by default.

Question 10 - Do you think that the FG covers the risks that may derive by the supply chain?

- ○ It covers too much.
- ○ It covers fairly.
- ◉ It covers fairly, but the tools and means shall be clearer.
- ○ It covers poorly.

5. Common Electricity Cybersecurity Level

Question 11 - Considering the 'minimum cybersecurity requirements' (with regard to Table 2 of the FG), select just one option:

- ○ They are applied to the right entities, they are proportional, and they fit with the purpose to protect cross-border electricity flows from cybersecurity threats.
- ◉ They are applied to the right entities, they are proportional, but they do not fully fit with the purpose to protect cross-border electricity flows from cybersecurity threats.
- ○ 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.
- ○ They are applied to the wrong categories.

Question 12 - Considering the 'advanced cybersecurity requirements' (with regard to Table 2 of the FG), select just one option:

- ○ They are applied to the right entities, they are proportional, and the fit with the purpose to protect cross-border electricity flows from cybersecurity threats.
- ◉ They are applied to the right entities, they are proportional, but they do not fully fit with the purpose to protect cross-border electricity flows from cybersecurity threats.
- ○ 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.
- ○ They are applied to the wrong category and entities.

Please, explain your reasoning for your answer to question 11 and 12, if necessary

600 character(s) maximum

The difference between minimum and advanced requirements is rather small and disputable - in particular the cybersecurity exercises which do not need to be exclusive - mat be structured and adjusted to all categories.
Additionally, the SMEs are neglected (as indicated before) - it is essential to have a reduced format of obligations and (supported) enforcement mechanism applied. The pattern should include (reduced sets of) cybersecurity rules for the energy Industry (in addition to certification), as well as for the suppliers and consumers (prosumers).

Question 13 - Please select the option(s) which in your view better represent how a common cybersecurity framework protecting cross-border electricity flows, should be established and enforced?

- ○ Through common electricity cybersecurity level that shall be certifiable by a third party (e.g. by the application of ISO/IEC 27001 certification).
- ○ The framework shall be based on a set of agreed requirements that shall be assessed, and their implementation shall be subject to governmental inspections.
- ○ A peer accreditation process shall be established, where electricity undertakings evaluate each other against a set of agreed requirements set by governmental authorities.
- ◉ A combination of those above.
- ○ Another better solution.

Please, briefly describe it:

600 character(s) maximum

The Item 1 (certifiable standards) appears as the most relevant and efficient - most adequate for the size and importance of the cybersecurity threat.
The Item 3 (peer evaluation among undertakings) is the closest to the source of the threat and most effective, enhancing the role and responsibility of the stakeholders (which is in their interest).
Governmental inspections are less credible. It may be effective to include the Energy Regulatory Authorities as enforcement agents.

Question 14 - 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

- [x] No

Please, explain why:

600 character(s) maximum

Transfer of essential services (those required for maintenance of the electricity flows) to a service provider de facto transfers the cybersecurity obligations / responsibilities to the (new) entity. For the sake of flexibility (which is relevant) such transfer should be possible and the answer is actually YES. There should be applied certification of the service provider for the specific technology, expertise and cybersecurity maturity, and monitoring of all the obligations transferred, and participation in all platforms for exchange of information.

6. Essential information flows, Incident and Crisis Management

Question 15 - 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 in order to:

- Provide agility to all electricity undertakings with respect to sharing and handling important cybersecurity information for cross-border cybersecurity electricity flows;
- Avoid interference and additional workload on the National CSIRTs and to their existing cooperation;
- Promote a responsible, autonomous, flexible, timely, coordinated and controlled approach to information sharing and incident handling, in line with current electricity practices and in line with the specific operational needs.

Considering the proposed approach, please select one option:

- [x] The proposed approach is feasible, can foster trust and provide enough flexibility and reliability, which are essential for the cross-border electricity flows.
- [ ] The proposed approach is feasible and can foster trust but it is not ideal for meeting the requested flexibility and reliability level.
- [ ] The proposed approach is feasible, but can hardly foster trust and it is not ideal for meeting the requested flexibility and reliability level.
- [ ] The proposed approach is not feasible, therefore needs to be reviewed.

Question 16 – The draft FG proposes the adoption of SOC to overcome other needs that go beyond the simple information sharing:
while it will offer the possibility to let the electricity sector to autonomously structure the information sharing infrastructure, ideally sharing resources and cooperating with the aim to reduce costs, offering high-end cybersecurity protection to cross border electricity flows, the same SOC may be delegated to other certain tasks for which a SOC is better placed in order to offer services (e.g. orchestrating cooperation with other CSIRTs, providing support in planning and execution of cybersecurity exercises, support and cooperate with critical and important electricity undertakings during crisis management situations and more);
Do you think that this secondary role is appropriate for the SOC?

- [x] Yes
- [ ] No

Question 17 - Do you believe a Cybersecurity Electricity Early Warning System as described in the proposed FG chapter 5.4 is necessary?

- (●) Yes, it is necessary.
- ( ) No, it is not necessary.

Question 18 - Concerning the obligation for essential electricity undertakings to take part to cybersecurity exercise as described in chapter 6 of the draft FG, please select one of the following options:

- ( ) It is in line with the objectives, and it contributes to the substantial improvement of the cybersecurity posture necessary for cross-border electricity flows.
- (●) It is in line with the objectives, and it contributes to the substantial improvement of the cybersecurity posture necessary for cross-border electricity flows, but the applicability should be extended to all electricity undertakings.
- ( ) It is in line with the objectives, but it does not really contribute to the improvement of the cybersecurity posture necessary for cross-border electricity flows.
- ( ) It is not in the objectives, and it should be abandoned.

Please, briefly describe the reasoning behind your choice:

600 character(s) maximum

There may be different level and format of exercises between the entities but the threats are shared and risk assessment mechanism must consider potential possibility of exposure and need for training across the landscape.
Furthermore, it should include the relevant entities across the borders with the Energy Community - assuming the very relevant need to enhance the protection from spill-over of the treat or cascading effects from an event in the highly interconnected network. The process of electricity market coupling between EU and CPs is advancing fast, and flexibility is increasing.

7. Protection of information exchanged in the context of this data processing

Question 19 - The proposed FG provides for rules to protect all information exchanged in the context of the data processing concerning the network code.
Considering the proposed rules and principles, please select one of the following options:

- ( ) The proposed rules and principles are appropriate and cover all aspects needed to secure the information exchanges in the context of the network code.
- (●) The proposed rules and principles are appropriate but miss some additional aspects needed to secure the information exchanges in the context of the network code.
- ( ) The proposed rules and principles are not appropriate and miss many additional aspects needed to secure the information exchanges in the context of the network code.
- ( ) The proposed rules are excessive, and a relaxation of rules and principles is suggested.

Please, describe the reasoning behind your choice:

600 character(s) maximum

Actually, the proposed rules and principles for data exchange miss a level of (possible) simplicity and effectiveness - they look too administrative and conservative with respect to confidentiality in some aspects. The process of "sanitation" could be simplified for some cases and the role of SOCs in exchange of information may be enhanced (they are the owners and most interested in the protection). Otherwise, the structure looks rather safe and robust.
In addition, for informal exchanges of information - platforms (ISACs) should be included in the scheme.

8. Monitoring, benchmarking and reporting under the network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

Question 20 - 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 appropriate and they cover all aspects needed to carefully monitor the implementation of the network code.
- ( ) The proposed monitoring obligations are appropriate but they do not cover all aspects needed to carefully monitor the implementation of the network code.
- ( ) The proposed monitoring obligations are not appropriate and they do not cover all aspects needed to monitor the implementation of the network code.
- ( ) The proposed monitoring obligations are excessive, and a major revision of the principles is suggested.

Question 21 - The proposed FG suggests benchmarking obligations to control the efficiency and prudence in cybersecurity expenditure, resulting from the implementation of the NC. Moreover, benchmarking, together with the identification of cybersecurity maturity levels of electricity undertakings, may constitute the grounds to further incentivise cybersecurity culture for cybersecurity electricity flows in the future.
In this respect, do you think that the benchmarking obligations are appropriate?

- (●) The proposed benchmarking obligations are appropriate and cover all aspects needed to monitor the efficiency and prudence in cybersecurity expenditure during the implementation of the network code.
- ( ) The proposed benchmarking obligations are appropriate but they do not cover all aspects needed to monitor the efficiency and prudence in cybersecurity expenditure during the implementation of the network code.
- ( ) The proposed benchmarking obligations are not appropriate and they do not cover all aspects needed to monitor the efficiency and prudence in cybersecurity expenditure during the implementation of the network code.
- ( ) The proposed benchmarking obligations are excessive, and a major revision of the principles is suggested.

Question 22 - 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.
Considering the proposed reporting obligations, please select one of the following options:

- ( ) The proposed reporting obligations are appropriate and cover all aspects needed to monitor the achievement of the objectives of the network code.
- (●) The proposed reporting obligations are appropriate but they do not cover all aspects needed to monitor the achievement of the objectives of the network code.
- ( ) The proposed reporting obligations are not appropriate and they do not cover all aspects needed to monitor the achievement of the objectives of the network code.

- ○ The proposed reporting obligations are excessive, and a major revision of the principles is suggested.
- ○ The proposed reporting obligations are very limited, and a major revision of the principles is suggested.

Please, describe the reasoning behind your choice:

600 character(s) maximum

The benchmarking should address all levels of entities (including SMEs, etc.) as indicated before - not only large and medium (essential and important) entities.

Question 23 - Do you think the proposed FG sufficiently cover cybersecurity aspects of:

	Partially covered	Fairly covered	Substantially Covered	Fully covered
Real-time requirements of energy infrastructure components.	○	○	◉	○
Risk of cascading effects.	○	◉	○	○
Mix of legacy and state-of-the-art technology.	○	○	◉	○

Question 24 - Do you have any other comment you want to share and that are not included in the previous questions, with regard to the rest of the content of the draft FG ?

1000 character(s) maximum

As indicated, there are aspects of cross-border cooperation in cybersecurity of the Member States with the Energy Community Contracting Parties which may contribute to better risk assessment, preparedness, resilience, cyber protection and maintenance of electricity flows across the EU perimeter borders (and hence in the EU as well). Such cooperation may enhance the overall level of cybersecurity in these systems - on mutual benefit, and this require special attention.
Notwithstanding the role of the FG addressing the EU geographic domain (and not third parties), and the need for background legislative framework required for its enforcement, there exist possible mechanisms and policies that may contribute to early implementation of the FG and the corresponding Network Code in these countries as well.

Contact

Contact Form