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

smartEn

* Type of business

Business association

Address

* Contact email

[redacted]

Phone

Country

BE - Belgium

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

We welcome the FG & its contribution to these objectives. However, more clarification is needed to assess the exact scope. The intention to cover a broad range of entities is welcome but uncertainty remains on the actual measures & their impact on the cybersecurity level. The parameters for classifying important/essential entities need to be detailed as it is difficult to assess the applicability of the minimum/advanced cybersecurity requirements and thus if a high common level of cybersecurity requirements will be applied broadly. Alignment with other EU legislation (e.g. NIS2) is also key.

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

Given that cyberattacks are quickly multiplying in number and in nature, the FG should ensure the NC aims at protecting the cybersecurity of the entire electricity system beyond the operational security of the T/D networks. This will support resilience of the overall service from end to end expected by consumers. The terms ‘cross-border electricity flows’ should be specified accordingly. Besides, the interoperability of cybersecurity requirements & standards should be addressed and supported in the NC. Aggregators not participating in electricity markets should also be included in the NC scope

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

The NC scope should clarify: 1) if it applies to entities of table 1 or only to those that can impact or be impacted by cross border flows & 2) how the ability to impact or be impacted by cross-border flows is assessed (under ECRI/ECRIC).Companies w/ large aggregation points connected to the system should be supervised/covered as they create the same risk level whether they participate in the electricity market/carry a supply function or not. (e.g. electro-intensive indus., EV charging point operators & essential service suppliers not established in the EU but delivering services in the EU).

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

We agree with the general objective of a quick implementation of the NC. However, the proposed transition period lacks clarity and transparency creating uncertainties regarding the classification process, its accuracy as well as on how to manage the passage to the long-term measures. The risks of essential entities under the transition period becoming important ones in the final system should be minimized as it can lead to unnecessary investments. Priority should be given to the implementation of the long lasting solutions foreseen in the NC.

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 right balance should be struck between costs/added value of cybersecurity measures. The index based on turnover & company size is not suited to classify small & micro-businesses as essential or important undertakings. Classification should be based on risk level as the only criteria for ensuring proportionality. For aggregators, this risk level should be linked to the size of their flexibility portfolio & other factors (e.g. assets type, connection type, reaction time). It should be clarified if ECRI & ECRIC apply to qualify the small and micro enterprise as essential/important entities.

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

The proposed governance is a welcome step with clear principles building on existing processes. Increased stakeholders' participation should be at the core of a sound governance in particular for the definition of the methodologies used to determine the scope of obligations for entities. Clarifications are also needed on the role and responsibilities for classifying entities. The autonomy of CSIRT need to be maintained and the support from specialists in cross-border electricity flows should be explicated and not lead to greater control from TSO/DSO.

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

Clarification is needed i) on who is responsible for the classification of important/essential entities and for ensuring stakeholders' involvement in the process; and ii) on who can trigger the reclassification of small and micro business which should be based on risk-level. A gradual phase-in of the final obligations should be preferred but in case the transition phase for the classification of entities is maintained, it should avoid stranded assets due to the reclassification of entities, be based on a transparent process with stakeholders and approved by ACER and not the Commission.

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

Further clarifications are needed on the responsibilities for running and implementing the ECRI for the classification of entities as well as for the identification and roles of specialists in cross-border flows in order to preserve the autonomy of CSIRT. It is also not clear who may grant the temporary derogations from the requirements of certification of the principles/minimum requirements and what criteria need be fulfilled, nor how these derogations would ensure high cybersecurity levels.

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

The high level methodology should be based on existing regulatory scopes (so as to reuse existing knowledge, tools) & on consequent stakeholder involvement. It should assess the investment required vs expected benefits and specify the frequency of the risk assessment. The list of threats should cover the specificities of new participants (e. g. risks of internet outages, cloud platform for VPPs, aggregators) and be shared across undertakings to foster synergies. The asset inventory should be required from all entities, whether they qualify as essential, important or small & micro enterprises.

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

We generally support the proposed obligations & allocation between entities. The obligations need to be proportionate based on the actual risk profiles of each undertaking. This can however only be assessed following a thorough definition and implementation of the ECRI and ECRIC used to classify entities, including small and micro business, as important or essential entities. These index should consider both the risk to which an electricity undertaking is exposed & the risk that this electricity undertaking could represent for other electricity undertakings and the whole electricity system.

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 NC should rely on existing and complementary families of standards, mapped through an equivalence table & certified by an independent third party. Thus the EPSMM involving stakeholder is welcome for defining the application of existing standards and levels and should support interoperability. "Maturity level" should be clarified as it does not guarantee a minimum cybersecurity level based on compliance with requirements/application of standards. Similarly, ECEMM should only be contemplated and on a voluntary basis as it would not provide minimum cybersecurity level based on certification.

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
- (●) No

Please, explain why:

600 character(s) maximum

The extension is welcome but obligations for essential entities & their role for imposing requirements to essential service suppliers (ESS) should be clarified. Extension to service suppliers of important entities could also be considered. Ambiguity for stakeholders both qualifying as essential entities & ESS should be lifted. A solution could be to apply the same regime (i.e. EPSMM). If maintained, cybersecurity certification schemes should carefully assess the use, impacts & costs of standards for the different actors & not push for a single standard. Product categories should be specified.

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:

- ○ 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.

Please, explain the reasoning for your choice (and if not feasible, explain the alternatives you would envisage)

600 character(s) maximum

The timing and requirements for disseminating data in case of major crisis, initial notification and reporting should be carefully assessed and be realistic and resource-efficient. The interaction and complementarity between SOC and CSIRT networks need to be further specified to avoid duplication, also in light of the NIS2 Directive. Besides, the Incident Classification Scale must lead to clear and harmonised incident qualification.

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?

- ○ Yes
- ◉ No

Please, provide your reasoning:

600 character(s) maximum

SOC should not be delegated the proposed tasks that go beyond information sharing which should be performed by CSIRTs also in line with NIS2 Directive. A further clarification of the SOC and CSIRT perimeters, roles and responsibilities in the FG would be welcomed to ensure that all actors have the same understanding of their respective roles.

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.

Please, provide the reasoning:

600 character(s) maximum

The implementation of a pan European ECEWS is a good initiative but should be supporting and consistent with the foreseen increased operational cooperation related to early warning in the CSIRT network under the NIS2 Directive, without creating duplication. The Framework guidelines should further specify how to implement the EU-wide ECEWS, in particular when it comes to governance, the application of the risk analysis before sharing information, the origin of the data to be used and the platform used to share information under the ECEWS.

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

Cybersecurity exercise are a good opportunity to improve the preparedness of the entire sector. The frequency of the mandatory internal cybersecurity exercise should be balanced taking into accounts its added value and costs/efforts. On some years, there will be an overlap with the mandatory regional cybersecurity exercise, creating an additional challenge for essential undertakings. Such frequency does not allow to sufficiently take into account the lesson learned. The proposed approach should be reviewed to make it more realistically implementable and affordable.

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

Trust is key for sharing information and is at the heart of the collaboration between CSIRTs. The NC should reinforce interlinkages with existing rules (REMIT, GDPR, protection of commercially sensitive & confidential info and of trade secrets). Rules for the definition of information ownership should not result in depriving legitimate owners of their rights on their information. The NC should give legal certainty as to the use of the information. The roles and identity of the 'processor' handling protected information should be clarified as it remains unclear who this is referring to.

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.

Please, describe the reasoning behind your choice

600 character(s) maximum

It will be important to regularly assess the effective contribution of the NC to the EU objectives on cybersecurity, taking into account technological advances and the changing nature of cybersecurity threats. However, it will be important that the scope of information to collect will remain within reasonable and achievable conditions for stakeholders and that the process to collect information will not create double reporting for all involved stakeholders.

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.

Please, describe the reasoning behind your choice:

600 character(s) maximum

The compliance with the NC provisions will require significant investments for undertakings. Assessing their efficiency and results answers to the legitimate electricity undertakings' concerns. It is welcome that the assessment looks at the potential adverse effects for the development of electricity systems and it should also consider potential barriers for the development of new business models. Such economic assessment should also be done in the case of transitional measures. The FG should specify how the results of the benchmarking will be used (e.g. for additional or updated measures).

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 publication of such report and the distribution of a “sanitized version” are welcome since the confidentiality of sensitive information is not an option in the cybersecurity field. The FG should further specify how stakeholders will contribute to the report and how this input will be taken into account. A close attention to consistency of cross-references between § 3.5.1 and 8.3 as well as the combination of provisions regarding the Cross-Border Electricity Cybersecurity Risk Assessment Report in the FG is needed.

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

smartEn acknowledges the paramount importance of a high level of cybersecurity for the energy sector in general, and for demand-side flexibility in particular. In order to be successful, innovative solutions need trust from society and politics.

smartEn supports the FG which stress the importance of the NC to be elaborated in a way that shall not constitute an unnecessary barrier to the access of new electricity undertakings and innovative solutions to the electricity market.

In this light, the relevant parties leading the drafting of the network code should involve stakeholders, including aggregators and new business models, in a structured and proactive way from the beginning of the process. This is the only way that the network code can provide an efficient answer to the challenges the grid, system operators and service providers are facing.

In addition, smartEn is asking ACER to set up an Expert Group as done for the DSF network code involving the relevant stakeholders.

Contact

Contact Form