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

EDF (Electricité de France)

* Type of business

Electricity generator and supplier

Address

* Contact email

[redacted]

Phone

[redacted]

Country

FR - France

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 ultimate objective of the FG could be clarified: there is a tension between the willingness to cover the involvement of a great number of actors and generally to reach a common and minimum cybersecurity level and on the other hand the establishment of what appears to be a very burdensome, detailed procedural framework. Clarification on the specific scope, terms used in the FG (including cross-border electricity flows and complementarities with other EU legislation on cybersecurity (e.g. NIS 2) will be a key enabler. So, the FG contribute to the 5 objectives but to an undetermined extent.

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

The FG mainly aim at ensuring the operational reliability and security of the electricity system but the security of digital connectivity and associated risks should also be recognized. A cyberattack against an electricity undertaking could lead to creating a weakness in the IT system used by a number of electricity undertakings without creating in this first instance any impact on the operational security of the electricity system. Such an impact would not be taken into account by the current NC scope of application but could be very detrimental in the long run.

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 adoption of a systemic approach that encompasses a large scope of actors of the electricity value chain is welcomed. The NC scope needs to be further clarified: (i) unclear whether the NC will apply to all entities mentioned in table 1 or only to those that can impact or be impacted by cross border flows and how the ability to impact or be impacted will be assessed, (ii) final customers such as electro-intensive industrial companies or CPO expected to be included in the scope as well as essential service suppliers not established in the UE delivering services to final customers in UE.

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

> Is a transitional period necessary? Resources mobilized, high uncertainty on the classification process and accuracy, no provision on how to manage the updates of categories. In the targeted situation, who will decide to classify an undertaking as an “essential or important undertaking”: a self-assessment and self-declaration process or a predominant role of the CS-NCA and NRA? No publication of the classification list for security reasons. The wording “essential” and “important” is confusing. Terms and definitions used in these different regulations to be differentiated if not same reality.

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

EDF Group supports a proportionate approach and support the principle of limited obligations for SME. The process to reclassify SMEs as important or essential (section 1.3) however needs to be clarified: who can trigger this process, what are the detailed applicable criteria (can they be made more sector specific), do the ECRI and ECRIC apply, is it clear that the SME becomes “important” or “essential” and thus has to comply with a new, larger set of obligations?

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

Key to reuse the existing governance, institutions, TCM approval process and increased stakeholders’ participation. Yet, the approval process of certain deliverables is too burdensome and time consuming: when NRAs or ACER have sufficient authority and greater technical knowledge, the EC should not be asked to approve. The support of CSIRTs by “a team of specialists in cross-border electricity flows” also raises concerns: does it mean that TSO/DSO or RCC experts will be involved in the CSIRTs of market participants? CSIRTs need to retain their autonomy and not be subjected to TSO/DSOs decisions

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

Three points on the classification: (i) Not clear how and who implement the ECRI to distinguish between essential and important, (ii) Not clear how to define and implement the ECRIC to requalify a SME as essential or important, (iii) Better to skip the transition phase and plan for a progressive phasing in of the long-lasting solution. Yet, if transition stays in NC, the transition list must i) not be approved by the EC (no sufficient knowledge); ii) be drafted with precaution (eg no demotion from “essential” to “important” in the final list, as it raises the question of stranded assets)

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

The FG need to:
- clarify who “all entities listed in Table 1” are: it can now refer to all or only part of the entities listed in the table
- clarify who may grant temporary derogations from the requirement of certification and what criteria have to be fulfilled. Is it ENTSO-E and the EU-DSO Entity?
- Clarify the roles and responsibilities of the “processor” in chapter 7. There is only one mention of this person in the FG: do we need such a person in the NC? Does it correspond to a specific business model? Or does it refer generally to entities of table 1 handing protected information?

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

An harmonised methodology at EU level needs to use existing governance models and be i) based on existing regulatory scopes (so as to reuse existing knowledge, tools and knowledge bases), ii) compliant with ISO 27005 (e.g. EBIOS or EBIOS RM), iii) based on a stable scope to prevent rework and iv) adapted for legacy systems with acceptable workaround measures (eg provision of long-term replacement roadmap). It must assess the investment required (time & materiel) vs expected benefits. The list of threats needs to be shared across undertakings to increase synergies and consistency.

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 allocation of obligations in the proposed Table 2 between the undertakings. However, a thorough and rigorous application of the ECRI and ECRIC will be required to ensure that SMEs with an impact on cross-border electricity flows are classified as important or essential and, generally, that all obligations are allocated to the undertakings depending on their level of risk.

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

We support the definition of a framework such as the EPSMM defining the application of existing standards and levels of "cybsersecurity controls". Using “maturity level” is misleading since it refers usually to the levels of the maturity methodology and is used for self-assessment but not for mandatory obligations. Not proven that the advanced cybersecurity maturity level is not present in an available standard and that the ECEMM will bring any additional benefit. ECEMM cannot bring guaranty by itself of a minimum cybersecurity level of electricity operators at European level.

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

It is good to extend the obligations to “essential service suppliers” for the cybersecurity of essential undertakings: should they also be extended for important undertakings?
Yet, it seems odd to provide for a different regime for essential or important undertakings (EPSMM or ECEMM) and “essential service suppliers” (EU Cybersecurity Certification Schemes and a standard mandatory by 2027). Outsourced products and services should be treated as if part of the undertakings’ assets and hence enter the scope of the risk assessment process, hereby including the supply chain.

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

Achieving within 20hrs max to anonymise, encrypt, send data across in case of major crisis is not realistic hence our reply above. The timings are far too short, same comment for the initial notifications & reporting. It is requested that SOC personnel join the CSIRT to cooperate in case of major incidents, yet it is also essential to limit this number to maintain active forces within the undertakings. The Incident Classification Scale (ICS) must lead to clear, easily understandable and harmonised incident qualification. It must build on the ENTSO-E ICS.

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

> We do not think that the SOC should be assigned the proposed tasks which should be performed by CSIRTs. A further clarification of the SOC and CSIRT perimeters, roles and responsibilities in the framework guidelines would be welcomed to ensure all actors have the same understanding. It would also be good to clarify whether CERT might exist as an alternative to CSIRT or whether they are always meant to be the same person.

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 seems necessary and is a good initiative as it should assist to enhance our proactivity in term of early detection of future attacks attempts. However, it will not be easy to implement: how will the correlation rules be defined? Risk analysis based, which ones? Where will the data to be used for such analysis be coming from? How secured will this platform be and how will it be securely shared with all actors? The governance and supporting models will have to be defined to make it as meaningful, useable and efficient as possible.

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

Taking part to such exercises will undoubtedly be beneficial, in particular in the context of cybersecurity trainings. However, the proposed frequency of the mandatory crisis exercise is too demanding in terms of costs and preparatory work. It does not either allow to take into account the lessons learnt. It is therefore not realistic. Exercises are thus in line with the cybersecurity objectives, but the proposed approach needs reviewing to make it realistically implementable.

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

The NC must clearly acknowledge the interplay with REMIT, GDPR and regimes for the protection of commercially sensitive & confidential info and of trade secrets. Data processing with built-in mechanisms ensuring compliance would foster a reliable flow of info between stakeholders and other entities accessing the info.
The NC is meant to contain rules for the definition of info ownership. It should not result in depriving legitimate owners of their rights on their info.
The rules for the secure transfer and treatment of info should build on existing reporting systems where possible.

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

We select answer 1 and wanted the opportunity to comment further:
EDF Group supports the establishment of a monitoring process. Indeed, in such a changing environment it will be important to regularly assess the effective contribution of the network code to the EU objectives on cybersecurity. The scope of information to collect should remain within reasonable and achievable conditions for 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

We select answer 1 and wanted the opportunity to comment further:
EDF Group supports the introduction of an economic assessment of the implementation of the NC. The compliance with the NC provisions will require significant investments for undertakings and assessing their efficiency, consequences and results answers to the legitimate electricity undertakings' concerns. The information related to cybersecurity expenditure remains in any case a sensitive information for the stakeholders.

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

We select answer 1 and wanted the opportunity to comment further:
EDF Group supports the publication of such report and the distribution of a “sanitized version” since the confidentiality of sensitive information is not an option in the cybersecurity field. We wonder how the stakeholders will contribute or be required to contribute to this report. 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

To complement question 13: We support ACER’s will to first establish a common minimum cybersecurity framework to be complied with by all electricity undertakings. The only way to ensure a common cybersecurity level is through the application of standards. The implementation of a maturity model, while allowing to improve the cybersecurity posture, does not guarantee a minimum cybersecurity level. That’s why we believe that the NC should focus on developing and implementing the EPSMM and remove any reference to “maturity” in relation to the EPSMM. This is only once the EPSMM has been duly and thoroughly implemented that the development of an ECEMM could be contemplated to promote a continuous improvement of each actor in terms of cybersecurity resilience. In any case, the ECEMM i) could never replace the EPSMM; ii) would need to be based on standards and iii) would have to remain a voluntary tool. It should comply to ISO/IEC 33004 and rely on ISO/IEC 27022 for process description.

Contact

Contact Form