eurelectric
powering people

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

A Eurelectric response paper

June 2021

Eurelectric represents the interests of the electricity industry in Europe. Our work covers all major issues affecting our sector. Our members represent the electricity industry in over 30 European countries.

We cover the entire industry from electricity generation and markets to distribution networks and customer issues. We also have affiliates active on several other continents and business associates from a wide variety of sectors with a direct interest in the electricity industry.

## We stand for

The vision of the European power sector is to enable and sustain:
- A vibrant competitive European economy, reliably powered by clean, carbon-neutral energy
- A smart, energy efficient and truly sustainable society for all citizens of Europe

We are committed to lead a cost-effective energy transition by:

**investing** in clean power generation and transition-enabling solutions, to reduce emissions and actively pursue efforts to become carbon-neutral well before mid-century, taking into account different starting points and commercial availability of key transition technologies;

**transforming** the energy system to make it more responsive, resilient and efficient. This includes increased use of renewable energy, digitalisation, demand side response and reinforcement of grids so they can function as platforms and enablers for customers, cities and communities;

**accelerating** the energy transition in other economic sectors by offering competitive electricity as a transformation tool for transport, heating and industry;

**embedding** sustainability in all parts of our value chain and take measures to support the transformation of existing assets towards a zero carbon society;

**innovating** to discover the cutting-edge business models and develop the breakthrough technologies that are indispensable to allow our industry to lead this transition.

Dépôt légal: D/2021/12.105/32

Working Group Technology
DSO Expert Group Cyber Security

Contact:
Caoimhin O BRIAIN, Senior Distribution Policy Advisor
cobriain@eurelectric.org

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

A Eurelectric Response Paper June 2021

## KEY MESSAGES

In response to ACER's Draft Framework Guidelines relating to a new Network Code on Cyber Security we have identified several key issues to be addressed, complementing our submitted response to the online survey, and due to limitations of the online format, under the following headings:

### Assets Based vs Process Based Risk Assessment

- We recommend using a combination of both bottom-up approach and top-down approach, i.e. asset-based and business process-based. The top down process based approach introduces a better overview of the real crown jewels of electricity undertakings which can affect cross border risk, and gives an overview over all interconnected systems and contacts. The combined approach will help address the weakness of each approach and reinforce them. That would allow i) reports to be made, ii) the identification of cyber risks and of the measures which could be adopted. The results of the top down, process-based approach could allow to input to definition of the ECRI and ECRIC and hence fine tune the classification of electricity undertakings.
- We believe, based on country specific experiences, that it is important to set requirements based on functionality and processes. The reason is that the processes may be the same throughout Europe, but the risk assessments included in the processes may be regulated by national law which currently prevents such information from being reported.

### Subject and Scope of the Network Code

- We recommend that the "size cap" for micro and small electricity undertakings be reconsidered. The number of employees is not a relevant measure, and neither is the number of customers. A relevant measure for producers also has to be defined, if they are deemed sufficiently large to impact security of cross-border electricity flows. The approach to include or exclude small and micro enterprises should be driven by risk parameters and demonstrable impact on the system in the context of security of cross-border electricity flows.

- Our concern is that rules on cyber-security will be defined in the network code, but its scope of applicability will remain unclear until either (i) development and implementation of a methodology on risk assessment and defining Electricity Cybersecurity Risk Index (ECRI) or (ii) transitional measures are adopted by the ENTSO-E / EU-DSO working group. This represents significant uncertainty for electricity undertakings. It may be prudent to plan for a progressive phasing in of the long-lasting solution, starting with the definition of the ECRI and ECRIC. In the meantime, electricity undertakings could continue with their current cybersecurity measures.

- It should be considered carefully whether the definition of "essential electricity undertaking" in the Framework Guidelines or other relevant notions (e.g., "essential business process" in the final informal report of the ENTSO-E and EU DSOs or "cross-border electricity flows" in the Electricity Regulation) that determines the scope of application of the network code should be defined entirely in the network code, or within subsequent methodologies required by the network code.

- There are doubts about the accountability of the process foreseen by the FG. While the cross-border risk assessment process under Section 1.5 and Section 3 is more inclusive than the transitional process under Section 1.6 none of the two processes guarantee due accountability. The cross-border risk assessment report will determine obligations of electricity undertakings; however, it is not subject to any regulatory or judicial review. Section 3.5.1 in point 13 indicates that the role of the Commission in the process will be limited to provide an opinion.

- Delegating the competence to define the scope of applicability through an implementation process may result in uncertainty and accountability issues. Please keep in mind the lengthy and complex process of implementing the Network Code Balancing.

## Verification of Compliance

- International standards or frameworks besides ISO/IEC 27001 shall be included and accepted as far as they have a way to measure them or be mapped to an existing standard.

- The approach of a "Maturity model" is completely different from the approach of "27001 certification" since the maturity model presents steps to implement "10 security domains and their objectives" which would not ensure a minimum security level among European energy operators, whereas ISO/IEC 27001 implies that the requirements of 27001, or other common mappable standards, are fully implemented (including controls to mitigate identified cybersecurity risks). It is not clear how it could be used.

## Information Sharing

- With regard to Question 15 and Question 16 on the Security Operation Centre (SOC): we agree with the objectives of the network codes on information sharing, smooth incident response or automated structuring of information sharing. However we are concerned about fixing all these functions to SOCs. The network code should foresee capabilities and functionalities of the electricity undertakings necessary for information sharing, however it should not prescribe the SOC as the one and only tool for such sharing , especially as those tasks should be performed by the CSIRTs. Moreover, even the small and micro

enterprises should have a responsibility to share technical information and it must go hand in hand with a responsibility to monitor and detect intrusions. Electricity undertakings must be obligated to identify risks and to detect threats even if they not have the capability to run a SOC. The requirements should be on functionalities and sometimes processes, not the specific set-up internally.

- It is unclear, how the Network Code on cyber security can add/complement obligations for electricity undertakings and existing national CSIRT's/EU-CERT/Coordination group/… regarding the topic of "Essential information flows, Incident and Crisis Management" (Chapter 5) on the existing 27 national implemented regulations based of the NIS Directive. Consistency between the Cybersecurity Act, the revised NIS 2 Directive and the NC is needed.

- A clear definition is needed when incidents are to be reported, as well as when feedback is given from CSIRT. The use of a standardised common taxonomy for cyber incidents as Mitre ATT&CK framework would support a rapid and stringent reporting. This allows the recipients of the shared information to be clear what kind of threat it is.

## Mandatory Product Certification

- Foreseen measures for mandatory product certification are far-fetched and may result in limiting the availability of ICT products on the market and restrain innovation. At the same time, the measures foreseen by the FG do not include measures that are easier to apply: introducing basic level of security for services and products, long-term security patches or standard contractual clauses that would improve the situation of electricity undertakings vis-à-vis the vendors.

- Voluntary certification of essential products should be considered instead of mandatory requirements. Product and measurements certifications are very far-fetched and may potentially result in limiting the availability of ICT products on the market and restrain innovation.

## General Issues

- Deviations of many of the principles in the Framework Guidelines from the Final Report recommendations of the Informal Drafting Team require further clarification. Meetings between the drafting team and ACER have been extremely fruitful in resolving many of these issues and are greatly appreciated.

- Please consider changing the name "essential service supplier" to "essential service provider", "digital service provider" or "vendor" as the term "supplier" can be confusing in the electricity context.

- We advise ACER to take into consideration the obligations which are already borne by electricity undertaking and to keep the overall framework coherent, efficient and as light as possible based on sound cost benefit considerations. The ultimate goal and focus of the sector is putting all the effort into contributing to enabling the transition to the carbon neutral economy and society by 2050, as stated in the Commission's Green Deal goals.

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 1pecialize 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

* Last Name

* Company/ Institution

* Type of Business

* Address

*Contact email

*Phone

*Country

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:

The FG contributes to major objectives. With its electricity asset approach, it may however miss some big cross-border cybersecurity risks originally targeted.

The intended scope of the network code should be set out as clearly as possible within the network code text, and the scope should be focused on security aspects of cross-border electricity flows based on accepted analysis. Local issues that do not contribute to security of cross-border electricity flows should be managed at a local level and in line with other relevant legislation.

600 character(s) maximum

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

- (●) Yes
- ( ) No

We agree that identifying a common set of rules for each relevant electricity undertaking is the only way to ensure a common minimum level of cybersecurity across European electricity undertakings affecting security of cross-border electricity flows.

However:

- The risk assessment should be based on processes & could be in combination with an asset based approach.
- The proposed asset inventory contains items not necessary for the further described risk management process.
- If necessary, the FG shall foresee a working group with participation of ENTSO-E & EU-DSO to tasks defined in the NC.

## 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

## 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

The FG provides for the establishment of a transitional list categorizing important and essential Electricity Undertakings. The companies will later be categorized by the ECRI method. Following the FG concept, some companies may be considered "temporarily" as essential and then be reclassified as important. Such uncertainty will not allow industrials to invest easily. Is a transitional period necessary at all or should resources be mobilised towards a progressive, phased in implementation of the targeted solution?

**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

## 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

**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

**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

## 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

**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

As long as we don't know which electricity undertakings will be categorised as important or essential, it is difficult to answer to these questions. We do not agree with just taking an Asset based approach - the approach should be based on critical business processes, as proposed by the informal drafting team.

The scope of application of requirements, within an electricity undertaking affecting cross border electricity flow security, needs to be clarified further.

**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

It should be clear, that only an agreed minimum baseline level for all grid participants would ensure protection for all grid participants. International standards or frameworks besides ISO/IEC 27001 shall be included and accepted as far as they have a way to measure them or be mapped to an existing standard.

The use of the terms Maturity, quality, level and effectiveness should be harmonized in the document to avoid ambiguities.

**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

## 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.

Mandatory information sharing solutions show less attractive performance than those shared in networks of voluntary trust. They lead to "minimum" participations. Moreover, it is surprising that companies under attack only have 2hrs to issue their alert where national CSIRTs experienced in the exercise have 18hrs to transmit the information. Public entities should pave the way to Electricity Undertakings and not the opposite. Regardless the obligation for national CSIRTs to transmit information within limited timeframes is welcome and fully responds to remarks made during previous consultations.

**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

The activity of SOCs should be devoted exclusively to defense and protection without having to deal with regulatory tasks, organisation of crisis exercises or other. Regulations should not interfere with internal business organisations. Therefore, we do not think that SOCs should be assigned the proposed tasks that should be performed by CSIRTs. Further clarification of the SOC and CSIRT perimeters, roles and responsibilities would be welcome to ensure all actors have the same understanding. Clarify whether CERT might exist as alternative to CSIRT or are they 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.

**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.

The pace seems ambitious, especially for national and regional exercises. Apart from a problem of synchronism in A+6, a more measured rhythm should be retained in the FG to remain realistic. In the PDCA spirit, each experience feedback from supranational exercise should lead to corrective and preventive actions. The NC can define the tool to monitor and ensure the achievement of these requirements, e.g European legislative texts.

The FG could mandate the NC to highlight activities which should be remunerated or financed. Securing cyber dedicated budgets will facilitate implementation of the NC.

## 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

To create a trust environment, protection of information exchanged according to its classification is a must.

Allowing ownership is omitted can help in some cases if National Authorities allow that.

The NC must clearly acknowledge the interplay with REMIT, GDPR and regimes for the protection of commercially sensitive & confidential information and of trade secrets. Data processing with built-in mechanisms ensuring compliance would foster a reliable flow of information between stakeholders and other entities accessing the information.

Rules should built 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.

Monitoring should be considered as a second step, once the implementation has started. 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 all 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.

Benchmarking should be considered as a second step, once the implementation has started. Compliance with the NC provisions will require significant investments for undertakings and assessing their efficiency, consequences and results is necessary to answer legitimate concerns of electricity undertakings. The information related to cybersecurity expenditure remains in any case a sensitive information for 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.

The reporting is an interesting concept. However, the FG should propose a more ambitious & dynamic process. We support the publication of such a report and the distribution of a "sanitised version", as the confidentiality of sensitive information is vital. We wonder how stakeholders will 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

A summary of our key messages is included in a separate email submission from cobriain@eurelectric.org , due to character constraints of the online survey format.

Eurelectric pursues in all its activities the application of the following sustainable development values:

Economic Development

- Growth, added-value, efficiency

Environmental Leadership

- Commitment, innovation, pro-activeness

Social Responsibility

- Transparency, ethics, accountability

Union of the Electricity Industry - Eurelectric aisbl
Boulevard de l'Impératrice, 66 – bte 2 - 1000 Brussels, Belgium
Tel: + 32 2 515 10 00 - VAT: BE 0462 679 112 • www.eurelectric.org
EU Transparency Register number: 4271427696-87