Summary and assessment of the Public Consultation PC_2021_E_04 on the Draft Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows

The Electricity Market Regulation provides the legal basis for the establishment of cybersecurity rules in the context of cross-border electricity flows. On 28 January 2021, the European Commission invited the European Union Agency for the Cooperation of Energy Regulators (ACER) to draft the Framework Guideline for a Network Code on Cybersecurity. On 29 April, ACER launched a public consultation ref. no. PC_2021_E_04 on its draft Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows (the "draft FG"), inviting stakeholders to submit their views to inform the finalisation of the document ahead of its submission to the European Commission at the end of July.

The Public Consultation ran between 30 April 2021 to 29 June 2021. This note provides a summary of the participants' observations and suggestions received and the reasons to accept or reject them in the revision of the draft FG. This summary also includes suggestions received during the consultation with the ACER's Electricity Working Group, most of which repeating some of the comments received during the public consultation phase.

1. Overview and general support to the draft FG

ACER received 42 responses to the public consultation. Most of the respondents belonged to the energy sector. On average, 35/42 respondents, equivalent to 84%, answered all the questions. The least answered question was Q8 on the potential for improvements in governance, with only 29/42 responses. Q19 on protection of exchanged information had the second lowest response rate with 32/42 responses, and the third were Q20 and Q21, on monitoring and benchmarking evaluation obligations, with a response rate of 33/42. On average, 24/42 respondents provided additional comments or reasoning to explain each of their suggestions, many of which are summarized in Table 1. In two separate cases, it appears that one respondent is part of the same organisational structure as another respondent.

Most of the respondents are positive to the proposed draft FG. 36/41 respondents, equivalent to 88%, believe that the FG contributes to the objective of further protecting cross-border electricity flows. The common feedback is that the FG contributes to the main expected objectives and that a network code is highly welcome. Only 5/41 respondents believe these objectives are not achieved with the proposal. 26/40 respondents believe there are still gaps concerning the cybersecurity of cross-border electricity flows, which the draft FG proposal should address.

Regarding the specific cybersecurity aspects for the electricity sector, 35/41 respondents, equivalent to 85%, consider that the proposed draft FG covers sufficiently the real-time requirements of energy infrastructure components, the risk of cascading effects and the mix of legacy and state-of-the-art technology. Only 15% consider it is covered partially.

2. Participants in the public consultation

Out of the total number of respondents to the public consultation, 35 stakeholders authorised the disclosure of their identity and contribution, while seven respondents asked for their submission to remain completely anonymous.

The majority of respondents to the public consultation indicated that they are based in an EU Member State, while four responses originated from stakeholders outside the EU (Switzerland, Norway, UK and USA). Stakeholders from Belgium submitted the largest number of responses (nine responses), followed by Germany (six responses) and France (four responses). A few responses to the public consultation were received from Sweden (three responses), Italy (three responses), Ireland (two responses), Netherlands (two responses), Slovenia (two responses) and Czech Republic (two responses). Other responses to the public consultation originated from Austria and Luxembourg (one response each).

The distribution of responses, received from a wide spectrum of stakeholders, is indicated below in Figure 1. Many responses (14) were received from business or industry associations, including associations representing energy exchanges; representing TSOs; representing DSOs; supply, distribution, sale and storage; power and heat generation; and cybersecurity for TSOs and DSOs. Nine responses were received by the energy industry, including TSOs, DSOs, electricity generators and suppliers, as well as energy production and DSO security. National competent authorities/national regulatory authorities submitted four responses. Non-governmental, non-profit organisations as well as a knowledge centre submitted three responses (one per organisation). Three responses were received by organisations representing exchanges (power and derivatives) and NEMOs. The remainder of the responses originated from diverse organisations, such as government bodies (two responses), security services companies (two responses), an IT services company, academia, an international organisation, an EU institution, a consulting firm and a company working on aggregation and virtual power plants (one response each).

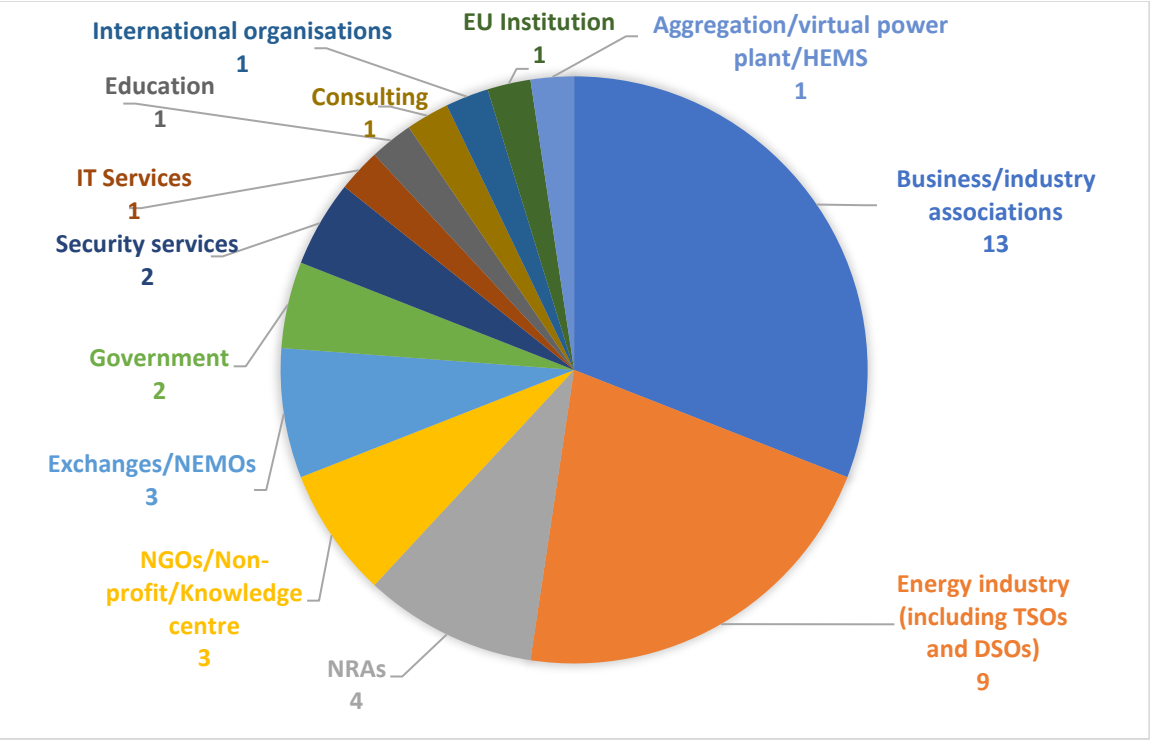

Figure 1 – *Distribution of the 42 responses*

3. Summary of opinions received

3.1. Meeting the general objectives

In general, most respondents consider that the draft FG contributes to the five objectives indicated in the consultation paper's first question. Most stakeholders (88%) responded that the draft FG contributes to the objective of further protecting cross-border electricity flows, in particular critical processes, assets and operations from current and future cyber threats. Similarly, a large majority of the respondents (90%) consider that the draft FG contributes to the objective of mitigating the impact of cyber incidents or attacks or of promoting preparedness and resilience in case of cyber incidents or attacks.

Most stakeholders (70%) also considers that the draft FG contributes to the objective of creating and promoting trust, transparency and coordination in the supply chain of systems and services used in the critical operations, processes and functions of the electricity sector. The majority of the stakeholders (85%) responded that the draft FG contributes to the objective of promoting a culture that aims to improve continuously the cybersecurity maturity and not to simply comply with the minimum level, as well as contributes to the objective of supporting the functioning of the European society and economy in a crisis caused by a cyber-incident or attack, with the potential of cascading effects (75%).

As a general observation, respondents explained that the specific scope of applicability of the draft FG as well as the requirements towards electricity undertakings should be further clarified. Similarly, stakeholders stated that the draft FG should not overlap with the NIS /NIS2 Directive, but rather complement it. Respondents highlighted that the scope of the draft FG should also include consumer assets, electro-intensive consumers, charging point operators and entities with an installed capacity of more than 1MW.

Two-thirds of the respondents consider that there are gaps concerning the cybersecurity of cross-border electricity flows, which the draft FG proposal should address. The remaining third of respondents consider that there are no gaps to be addressed in the draft FG. Some of the gaps identified by respondents are the applicability/scope of the network code, definitions of legacy systems, random security audits, excess of disclosure of information, consideration of the high degree of interdependencies with other critical sectors, reasoning for 8h/10h/20h, etc. and ask to provide a short summary in each chapter explaining the goal of the focus areas.

3.2. Scope, applicability and exemptions

Stakeholders' opinions are divided regarding the applicability of the Network Code. Half of the respondents consider that the applicability proposed in the draft FG covers all entities that may have an impact on cross-border electricity flows because of a cybersecurity incident/attack. The other half consider that not all entities are covered and ask for more clarity on the scope of applicability of the network code (Table 1 in the draft FG) and propose additional entities to include, such as electro-intensive industrial companies or charging point operators, essential service suppliers not established in the EU delivering services to final customers in the EU, relevant service providers with equipment connected behind the meter, manufacturers of consumer equipment, such as solar inverters, brokers, etc.

3.3. Classifications of applicable entities and transitional measures

The draft FG proposes that all small and micro-businesses, except those that are defined as important/essential electricity undertakings, shall be exempted from the obligations set in the

NC, excluding the general requirements for cyber hygiene. Half of the stakeholders responded that this approach is consistent with the general idea to uplift and harmonise the cybersecurity level within the ecosystem to efficiently protect cross-border electricity flows, while the other half disagree arguing a lack of clarity on when and which authority will be responsible for this classification as well as the inadequate rule applied based on size/turn-over and not on the risk level and activities carried out by these companies.

The proposed draft FG prescribes a process to differentiate electricity undertakings based on their level of criticality/risk. This will imply a transition period of two years until the full system is established and will require the establishment of a proper governance to duly manage the entire risk assessment process. One-third of the stakeholders consider that the proposed transition is the most adequate, while the other two-thirds disagree with the proposed transition period. The arguments are quite diverse, e.g., transitional phase is not needed as the NIS2 Directive will soon be implemented; or that the proposed transition approach may cause that some entities transitionally classified as essential might later be identified as important, which could cause uncertainty in terms of investment.

3.4. Cybersecurity governance

Stakeholders' answers were split regarding the governance for the overall process of ensuring the cybersecurity of cross-border electricity flows. 46% consider that the draft FG succeeds in establishing a sound governance for the overall process of ensuring the cybersecurity of cross-border electricity flows, whereas 54% disagree and indicate interesting recommendations on key topics, summarized in Table 1.

Two-thirds of stakeholders responded that the decision on setting the conditions is assigned to the correct decision group, while one-third consider that the decision should be taken at a higher strategic level in respect to what is proposed in the draft. They highlight that clarification is needed on who is responsible for the classification of important/essential entities and for ensuring stakeholders' involvement in the process as well as who can trigger the reclassification of small and micro businesses which should be based on risk level.

3.5. Cross border risk management

Stakeholders show two main preferences for the risk management methodology for assessing and managing risks of cross-border electricity flows. While 56% of stakeholders support the proposed bottom-up methodology based on three consecutive levels, 38% of the participants, mainly system operators, declared their preferences for a top-down approach.

Regarding the risks that may derive from the supply chain, 81% of stakeholders consider that the draft FG fairly covers these risks but half of them recommend further clarity of the tools and means in the final network code.

3.6. Common electricity cybersecurity level

Almost all respondents (98%) believe that the minimum cybersecurity requirements from Table 2 of the FG are applied to the right entities and fit fully or partially with the purpose to protect cross-border electricity flows from cybersecurity threats. Only 2% think that they are applied to wrong categories, arguing small and micro entities should be covered to a larger extent by the FG. Regarding the proportionality of the minimum requirements, half of the respondents believe they are proportional, while the other half believe they are not, with 20% arguing that the

methodology for classification of entities and whether they should be subject to minimum or advanced requirements shall be further defined.

A large majority (88%) of respondents believe the advanced cybersecurity requirements from Table 2 of the FG are applied to the right entities and fit fully or partially with the purpose to protect cross-border electricity flows from cybersecurity threats. Only 10%, mainly related to the TSOs' opinion that RCCs shall not have a risk management role, believe that the requirements are applied to wrong categories. Regarding the proportionality of the advanced requirements, 56% of respondents believe they are proportional, while 32% believe they are not proportional.

Additionally, 92% of respondents support the establishment and enforcement of a common cybersecurity framework that protects cross-border electricity flows, but there are three different but equally supported preferences for the compliance process: through the certification of a third party (for example, applying the ISO / IEC 27001 certification); based on an agreed set of requirements and subject to government inspection; and a combination of the two previous alternatives.

Regarding the proposed obligation of cybersecurity measures and standards for essential service providers, 64% of respondents believe that this is the correct approach, while 36% believe that it is wrong but many of them could support it if the requirements were to be clarified in the network code.

3.7. Essential information flows, incident and crisis management

The FG proposes to use the designated capabilities of the Electricity Companies Security Operations Centre (SOC) to enable seamless information sharing and incident response. 70% of respondents believe that the proposed approach is feasible and can build trust, while the other 30% believe that it is not feasible, expressing concern about the short time frame of 20 hours to share information or suggesting strengthening the CSIRTs instead.

43% of respondents believe that SOCs should support other needs that go beyond simple information sharing or a secondary role in crisis management, cyber exercises, and orchestrating cooperation with CSIRTs. In contrast, 56% of respondents do not believe that this secondary function is appropriate, arguing that SOCs should not receive tasks from CSIRTs because it should not necessarily be performed by a SOC and will lead to repetition of reporting

85% of respondents believe that a Cybersecurity Electricity Early Warning System is necessary as described in chapter 5.4 of the proposed FG. The remaining 15% are not against it but are concerned if it is aligned with NIS2 or think the proposal needs further clarification.

All respondents believe the obligation for essential electricity undertakings to take part to cybersecurity exercise is in line with the objectives of the FG. Two-thirds of respondents believe the obligation contributes to the substantial improvement of the cybersecurity posture necessary for cross-border electricity flows. 20% of respondents are critical to the exercise frequency proposed in the FG and ask for more time to evaluate lessons learned and implement changes and keep costs at an acceptable level.

3.8. Protection of information exchanged in the content of this data processing

80% of the opinions received consider that the principles proposed in the FG are adequate and cover all the necessary aspects to ensure the exchange of information in the context of the

network code. On the other hand, 28% of those surveyed consider that some additional aspects are missing to ensure the exchange of information, such as aggregated data from small devices, rules to define the ownership of information, interaction with REMIT, GDPR and regimes for the protection of sensitive business information and trade secrets, etc.

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

82% of the responses consider that the proposed monitoring obligations are appropriate and cover all aspects needed to carefully monitor the implementation of the network code. The remaining responses think that it does not cover all aspects needed but agree with the regularly assessment of the effective contribution of the network code to the EU objectives on cybersecurity.

70% of the responses consider that the proposed benchmarking obligations are appropriate to monitor the efficiency and prudence in cybersecurity expenditure during the implementation of the network code. They welcome the introduction of an economic assessment but highlighted that the information related to cybersecurity expenditure is in any case sensitive information for the stakeholders and shall be treated as confidential. 30% suggested not to focus solely on the cybersecurity expenditure but also consider the overall maturity of cybersecurity measures in place. Only 23% believe that benchmarking obligations are excessive and suggest a major revision of the principles.

According to 72% of the opinions received, the reporting obligations are clear and will help the monitoring objectives. On the contrary, 23% believe that the reporting obligations are excessive and suggest conducting a gap-analysis to ensure efficiency and prevent unnecessary reporting duplications. TSOs are of the opinion that the role of RCCs should be excluded from these reporting tasks due to their lack of expertise, skills and IT solutions; furthermore, they reminded that the description and mandate of RCCs as given by the Directive 2019/943 does not enable them to undertake such tasks.

4. Main observations retained

The consultation was extremely useful, with very good suggestions both in quality and quantity, many of them have been incorporated into the revised version. Annex I summarizes most of these suggestions and the reasons for their retention or rejection in the revised FG.

Annex I - *Suggestions received and the reasons to accept (A) or reject (R) them in the revision of the draft FG*

Section in FG	**Suggestions received**	**A/R**	**Reasons to accept or reject**
N/A	As a general remark, one stakeholder suggested adding a short summary in each chapter explaining the goal of the focus areas.	A	The revised draft FG includes a box at the end of each section with a summary of all the deliverables for that section and responsible entities, which should add clarity regarding the goals of the NC.
N/A	The FG should include details on the application to connected non-EU countries and reference as to related non-EU aspects of cybersecurity	R	This suggestion covers aspects that would be out of scope of the FG. The draft FG includes details on the applicability of the NC to entities established in third countries operating in the EU.
N/A	Regarding the aspects that may be developed further, two stakeholders recommended the use of the definitions, applicability and physical coverage that currently exists in the system operation regions (SOR), using and adapting the SOR concept inside the FG, instead of creating new cybersecurity regions.	A	The draft FG was revised to refer to SORs instead of the originally proposed cybersecurity regions.
N/A	Regarding the governance aspects proposed in the draft FG, two stakeholders consider that national competent authorities should have a role in supervising cybersecurity requirements.	A	The revised draft FG takes into consideration this comment for cases where either the CS-NCA or NRA is responsible for supervising cybersecurity requirements due to national legislation.
N/A	Four respondents mentioned that the role of the RCCs should be reconsidered.	A	The draft FG was amended to reflect the views of stakeholders, instead attributing the role to ENTSO-E, in cooperation with the EU DSO entity and RCCs.

1.2-1.3	Stakeholders suggested more clarity in the specific scope of applicability (e.g., NEMOs, exclusions for small and micro entities, etc.), terms and definitions used (e.g., essential and important electricity undertakings), and ensuring consistency with other EU legislation on cybersecurity.	A	The draft FG has been thoroughly revised to better clarify: - The scope of applicability, by introducing changes to Table 1 (including an explicit reference to NEMOs) and throughout the text with reference to the entities the NC shall apply to and adding clarity regarding small and micro entities; - The terms used, by changing the wording regarding essential and important electricity undertakings so that there is no confusion with the wording used by the NIS2 Directive; and - The definitions used in the document, by fully revising their contents to ensure consistency and by adding definitions that were necessary to correctly understand the draft FG.
1.3	Regarding the draft FG's process and governance to determine the conditions to classify and distinguish electricity undertakings, four stakeholders advocated for the use of existing lists such as those under NIS2 and relevant national legislation.	R	The draft FG was amended to fully align this classification with the lists in the proposed NIS2 Directive. The entities listed in Table 1 of the FG represent the major stakeholders, which may affect cross-border electricity flows directly or indirectly.
1.3	ACER was requested to carefully consider the scope of the Framework Guideline, in particular the inclusion of NRAs within the scope of the Framework Guideline. All entities in Table 1 are affected by the network code, but not all have the same obligations. It is suggested to clarify this when establishing Table 1, particularly the role of the NRAs.	A	According to chapter 1.3 in the proposed FG, the network code will apply to the public and private entities listed in Table 1 (called "entities") that may affect cross-border electricity flows directly or indirectly. This includes NRAs. However, the common electricity cybersecurity framework may not be applicable to NRAs or other entities who can show through the proposed risk assessment that they may not directly or indirectly affect cross-border electricity flows. To clarify this, the rules in chapter 4.1 have been updated, giving CS-NCAs and NRAs a clear right in such cases to issue derogations for maximum two years for any entity in Table 1.

1.3	Regarding applicability of the network code, intensive consumers/ final customers such as electro-intensive industrial companies or charging point operators / small production units should be included.	R	Rather than going the last mile at the end user, the draft FG includes energy aggregation and storage as initial entities relevant to the cybersecurity aspects of cross-border electricity flows. Still, as explained in the following comment, the FG foresees the possibility for entities not initially listed in Table 1 to be eventually included in the list, should it turn out that the latter have an impact on cross-border flows.
1.3	There are entities not listed in Table 1 who may have a large impact on cross border electricity flows, e.g., large industrial consumers.	A	Chapter 1.3 has been updated so that stakeholders who are not listed as entities in Table 1 may still be nominated to be covered by the network code, like the process for small and micro entities.
1.3	According to NIS2, the network code should foresee the possibility of applying it to small and micro enterprises, but not only under the initiative of any company listed in Table 1.	A	The revised FG introduces additional conditions for this case: the network code must provide for the possibility of applying it to small and micro-enterprises at the initiative of any entity listed in Table 1, after consulting and having obtained an opinion from the competent NRA and the CS-NCA
1.3	The exclusion of small and micro-businesses is inadequate if based on size/turn-over and not on the risk level and activities carried out by these companies.	-	In line with the proposal for a NIS 2 Directive, the network code could also apply to those small and micro enterprises that cover specific high-risk or critical roles in the cybersecurity value chain of cross-border electricity flows.
1.5	Regarding access to information, NRAs usually have access to sensitive information, but not confidential information in the cyber domain. Not all NRAs have security clearances at Member State level.	A	The draft FG was revised and the word "confidential" was changed to "sensitive". It also expanded the clarification in the event that an NRA does not have security clearances at the Member State level, indicating that in that case, the CS-NCA will grant the NRA relevant access to information based on the "need to know”.
1.5	Regarding newly created or existing entities that provide new services under the classification shown in Table 1, the network code shall not be an obstacle for new entities by imposing conditions prior their start-up. It is suggested to define deadlines to comply with the network code.	A	The draft FG was amended to reflect these views. Rather than subjecting the start-up to the execution of an inventory of assets and a risk assessment, the revised FG allows starting the operation of new entities or services and presenting the asset inventory and risk assessment within the first initial year of operation. This period may be shortened if deemed appropriate by the CS-NCA and NRA based on the risk assessment.

1.6	The proposed transition approach may cause that some entities transitionally classified as essential might later be identified as important, which could cause uncertainty in terms of investment.	A	The revised draft FG proposes that the transitional list shall be based on a precautionary principle, so that entities may only gain more responsibilities in the revised list after the end of the transition period, compared to where they stand in the transition list (e.g., no demotion from “critical” to “high-risk” in the revised list).
1.6	Five respondents highlighted that the proposed transition approach could cause uncertainty; two stakeholders mentioned that it should be more comprehensively developed; two stakeholders stated that the proposed transition period lacks clarity. Three respondents stated that sufficient time should be given for the transition.	A	The wording regarding the transition phase has been revised to add clarity and avoid uncertainty to the process.
2.1	The FG shall ensure that the network code does not overlap with NIS / NIS2, but rather complements it.	A	The FG draft was modified to reflect this principle and introduced it within the framework of the "General Principles": the network code should complement and be consistent with the two proposed Directives on measures for a common high level of cybersecurity across the Union (NIS2) and the resilience of critical entities.
3.2	System Operators recommend a top-down Business Process Risk approach to cyber risk identification, evaluation and treatment, rather than the asset management bottom-up approach recommended by the FG. Taking the critical business processes as starting point for risk assessment will be both more efficient and effective.	A	The revised draft FG proposes an integrated top-down and bottom-up cybersecurity risk assessment methodology and asks the network code to ensure the complementarity, governance, and flexibility of both existing methodologies. The top-down approach will be used for the transitional list.
3.2	Four stakeholders suggested establishing a working group with the participation of ENTSO-E and EU DSO entity.	A	The network code shall ask ENTSO-E and the EU DSO entity to establish a top-down risk assessment working group for the top-down risk assessment methodology.
3.3	Harmonised principles should be promoted for Assets Inventory and Electricity Cyber Perimeter definition	A	The revised draft FG asks the network code in section 3.3.1. to set rules to clearly identify individual assets in a harmonised way and create asset inventories of each ‘high’-risk and ‘critical’-risk electricity entities as well as define the methodologies and tools to define an electricity cybersecurity perimeter.
3.3	What is the point of managing two separate asset inventories for critical-risk and high-risk entities?	A	The text has been adjusted to clarify there shall only be one asset inventory per entity.

3.4.	The FG should consider the interdependencies with other critical sectors.	A	As part of the Reporting process, it is proposed that the Cross-Border Electricity Cybersecurity Risk Assessment Report shall be submitted to the NIS Coordination Group for further analysis, in particular in order to identify crucial interdependencies with other sectors where an additional level of harmonisation may be needed.
3.4	For consistency between specific new cybersecurity risks and the RP cybersecurity scenarios, National Competent Authorities for Risk Preparedness should participate in the cross-border risk assessment.	A	The FG establishes the main responsibilities. In general, CS-NCAs, RP-NCAs and NRAs shall be responsible for aggregating assets inventoried and risks analysed in the first level of risk assessment and reporting to the regional level. ENTSO-E, in cooperation with the EU DSO entity and the RCCs, shall be responsible for activities at the third level of cybersecurity risk assessment. RP-NCA will be consulted and actively participate in the interface between the first and the second as well as between the second and the third levels.
3.5	Regarding the transitional phase proposed in the draft FG, a few stakeholders stated that a transitional phase is not needed as the NIS2 Directive will soon be implemented and one stakeholder questioned whether a transition period is at all needed.	R	The transition phase is needed to facilitate the implementation of the network code using existing methodologies for cross-border risk assessment purposes until the final methodology is defined and delivered during the first two years after the entry into force of the network code.
4.1	Regarding the verification of a common cybersecurity framework, a quarter of respondents from various categories of entities prefer third-party certification as the only methodology.	R	By choosing a combination of certifiable or verifiable standards, government inspections and peer accreditation processes, the revised draft FG proposes Member States can decide themselves which scheme(s) to apply.
4.1	Regarding verification of a common cybersecurity framework, respondents from various categories of entities prefer a combination of the use of certifiable or verifiable standards, government inspections and peer accreditation processes.	A	The revised draft FG introduces the choice of strategy to verify a common cybersecurity framework, which adds flexibility to the verification process and opens the door to continued use of schemes already implemented in the Member States.
4.1	One fifth of respondents from various categories believe that the roles and responsibility of the entities needs to be further clarified, e.g., what is part of the minimum requirements.	A	The text regarding a common cybersecurity framework is clarified in the revised draft FG. The detailed requirements shall be further clarified in the network code and based on the results of the risk assessment.

4.2	Who shall run the proposed penetration tests (in the absence of certification)?	A	The text has been adjusted to clarify that the entity responsible for the critical process (the critical-risk entity) shall be responsible that such a test will be conducted, and that penetration testing may be executed by the critical-risk entity, by authorities, by commercial or academic organisations or any other entity the critical-risk entity may find suitable for the task.
5.1	Some member states have national laws prohibiting sharing of incident related information. There may also be situations where sharing incident related information may be harmful.	A	The revised draft of the FG allows CSIRTs to withhold information and request advice from ACER and ENISA in cases where dissemination at the EU level is considered a risk.
5.1	The sentence "The network code may apply own rules connected to the participation of small and micro enterprises" is too vague.	A	Another sentence has been added saying "Such rules shall aim to reduce cybersecurity risk following participation of small and micro enterprises as these may not be subject to the common electricity cybersecurity framework and therefore may have a lower cybersecurity standard than the high-risk and critical-risk entities"
5.1	Who will define the processes and technologies and ensure daily operations?	A	The text has been updated and now suggests that since the CSIRTs on Member State level will be a central part of the information sharing network, they may define processes and technologies and ensure daily operations.
5.1	Will the information sharing mesh networks be part of the ECEWS?	-	The interaction between the information sharing networks and ECEWS is described in chapter 5.2.
5.3	CSIRTs should be strengthened rather than requiring SOCs	R	The draft FG refers to CSIRTs as entities operating on national level and SOCs at entity level, although CSIRTs may be used for SOC tasks on entity level as well. How to organize this will be up to the entities. The objective is that the entities will have the capabilities to follow up cyber-incidents.
5.3	SOCs should not be given tasks beyond information sharing. One of the arguments is that SOCs should not be given tasks of CSIRTs	R	The draft FG makes it clear that the CSIRT can handle incidents, if that is what the entity prefers. In this sense, it is understood that there is an overlap between the tasks of the SOC and the CSIRT.
6	Reduce the frequency of the proposed exercise to have more time to evaluate the lessons learned and implement changes and keep costs at an acceptable level.	A	The revised draft FG proposes to reduce frequency of internal exercises from two to three years.

6	ACER was asked to confirm that the exercise concerns only critical-risk entities and not NRAs.	R	If an NRA, after the risk assessment, is defined as critical-risk entity, we suggest the NRA should also be part of the cybersecurity exercise.
7	Make sure that all information exchanged in the entire chain is protected by the rules proposed in the draft FG.	A	Already covered by the current draft FG
7	The rules for the classification of the information exchanged should be defined in the context of the network code.	A	Already covered by the current draft FG
7	The network code must clearly acknowledge the interplay with REMIT, GDPR and regimes for the protection of commercially sensitive & confidential info and of trade secrets.	A	The revised FG states that any provisions of the NC on confidentiality and protection of data shall be without prejudice and in line with existing legislation for the protection of commercially sensitive, confidential information and trade secrets. In particular, the NC shall be fully aligned with REMIT and GDPR.
7	ACER and ENISA have no mandate to decide on litigation over classification, or about the refusal to process or exchange information involving entities from more than one Member State. ENISA proposed that the Commission shall decide.	A	Rather than ACER and ENISA, the NRAs shall decide on litigation over classification, process or exchange of information involving entities from more than one MS.
8.1	ENTSO-E and the EU DSO entity to conduct a gap-analysis to ensure efficiency and prevent unnecessary duplications of the reporting obligations	A	The revised draft FG highlights in section 8.1 that the information gathering process shall be kept in reasonable and achievable conditions, minimising the efforts of all stakeholders involved and avoiding double notification by the electricity entities and their associations.
8.1	ACER's monitoring tasks should focus on monitoring the implementation of the legislation and not on monitoring compliance.	A	In the revised draft FG, ACER is not tasked with assessing compliance and measuring maturity, but the other monitoring activities are maintained.
8.1	If too many organisations are expected to carry out the same activities at the same time, the chances are high that there will be inefficiencies, inconsistencies and delays. Only one authority at a time should have oversight for specific operational tasks like the ones described here.	A	The text has been updated to specify that ACER has the main responsibility of conducting the monitoring. However, ACER depends on cooperation with ENISA and support from ENTSO-E and the EU DSO entity to be able to monitor areas where ACER do not have the specialised cybersecurity competence.

8.2	The information related to cybersecurity expenditure remains in any case a sensitive information for the stakeholders.	A	The following text was added in chapter 8.2: “Information related to cybersecurity spending shall remain confidential information and shall be managed jointly and securely by the CS-NRAs and NRAs at the national level and ACER and ENISA at the European level.”
8.3	Shall the risk report include listing systems with lowest level of security (since it asks for system with highest level of security to be listed)?	A	The text has been updated to include also systems with lowest level of security.
8.3	The reporting obligation is not in line with some national laws, which can prohibit sharing certain info. The proposed FG has several clauses where information would be reported and/or gathering where the information may be of a security sensitive nature, or when combined and aggregated with other data.	A	Compliance with national laws, confidentiality and sensitivity issues seems to be well covered in the present draft FG, which foresees that the report shall be subject to the rules on protection of exchange of information described in chapter 7 and released in a sanitised public version after approval by the NIS Coordination Group.
8.3	The reporting obligations are clear and will help the monitoring objectives. The role of RCCs should be excluded from these reporting tasks, due to the lack of expertise, skills and IT solutions. Also, the description and mandate of RCCs as given by the Directive 2019/943 do not enable them to undertake such tasks.	A	RCCs were removed from the reporting tasks in section 8.3 of the draft FG.