Contribution on the cybersecurity network code draft submitted to consultation by ENTSO-E

Paris, 8 December 2021

The EDF Group welcomes the significant work on the draft network code on cybersecurity (NC) which was accomplished by the drafting team under significant time pressure. We also welcome that stakeholders could contribute through a drafting committee. At this stage, this draft NC is covering most of the topics mentioned in the ACER Framework Guidelines (FG). We nevertheless consider this draft to be far from finalisation. Though we support the current text and believe that it should serve as the basis for further work from all involved parties, we believe that too many critical elements still require clarification. Some significant interpretation gaps remain wide open for practitioners so that provisions could be effectively implemented. A number of critical issues still revolve around questions of governance and questions on the feasibility to implementing the different processes and measures foreseen in the NC. Among others, some of those issues in the NC pertain to:

(i) **The timing for adoption**. It would be detrimental to adopt the NC provisions before the adoption of the NIS2 Directive. It is of the utmost importance to ensure that the concepts, terminology and requirements of both texts are aligned, especially with regard to requirements on information flows, incidents and crisis management. An extension of the NC drafting timeline would also allow drafters and contributors to properly address the remaining blocking points and ensure the quality and enforceability of the draft. Significant work is still required to design the most relevant, consistent and efficient cybersecurity legal framework for the electricity sector. This is not achievable within the current 14 January 2022 deadline.

(ii) **The many open questions regarding the implementation.** As things stand, the NC obligations are undecipherable for many actors. For example within the currently proposed risk assessment cycle, it is not possible for an entity to confidently determine what its obligations are, nor when and how to effectively comply with them. Developing all the required deliverables within the two years' timeline does not either seem realistic.

(iii) **The unclear scope of application**. The NC needs to clarify who is falling under its scope: some actors are well identified but the question remains open for other actors. It is a key factor to reach the objective of an increased cybersecurity in the electricity sector.

(iv) **The unprecise nature of many critical parameters**. Stakeholders should not sign a blank cheque and commit to implement a NC whose critical parameters are not yet defined. An unchecked and unmonitored working group should thus not be given the power to decide on so many critical elements of the future cybersecurity framework. All methodologies developed by the ENTSO-E and the EU-DSO entity must be approved by the competent regulatory authorities: the regulatory power should not be delegated to ENTSO-E, the EU-DSO entity or the working group. The NC should also clearly specify the objective and intended content of the methodologies to direct and funnel their development.

(v) **The lack of a clear plan for IT tools for information exchange and early warning**. Though we understand that time is required to develop such tools and that they could not be available as from the entry into force of the code, we need to have more certainty on their development, their financing, their functioning modalities and own cybersecurity and privacy protection. We also need a credible timeline for their commissioning and indications of the rules to follow in the absence of such critical tools (before their development or as a fall-back).

This contribution is meant to complement the EDF's Group answer to the public consultation organised by ENTSO-E and EU DSO entity on the draft NC.

1. General comments

As an introduction, we would like to draw your attention on three points relating to the legal drafting and robustness applying throughout the draft NC:

(i) The obligations need to be properly allocated. Obligations could be allocated to several entities, such as "*the ENTSO for Electricity and the EU DSO entity*", only when each entity is expected to comply with the obligation on its side. Even in that case, the obligations must be reviewed to make sure that they do not lead to unintended consequences: the current drafting of article 8 could lead to organising two public consultations on a same deliverable, which would not be useful. However, a single obligation cannot be allocated jointly to several entities, unless there is a specific decision making governance established: what would indeed happen in case those entities cannot agree on how to perform the obligation? It is preferable to set the obligation only on one entity, with the possibility or obligation for this entity to consult the other: for instance ENSTO-E could be vested with obligations which it would have to perform, in coordination with the EU DSO entity.

(ii) The obligations must be set on actual natural or legal persons, which is not currently always the case: e.g. in article 19(1), the "*risk assessment*" cannot be the subject of obligations; article 2(2)(c) needs to specify who should be in charge of classifying SMEs by application of the index.

(iii) The consistency of the terminology should be ensured. For example, the use of the term "entity" should be reviewed. Sometimes it refers to "*high impact entities*", to "*critical impact entities*", to both or to a third category of persons. More generally, the definitions in article 4 must be reviewed to ensure that they are consistent with one another and with the already existing legislation (especially if listed in article 4(1)) but also that they are necessary (not used only once or being straight forward terms), standalone and not circular.

2. Scopes and objectives

We consider that article 2 on the scope still raises many questions. We can list among others:

(i) Electricity digital market platforms: does the definition mean that the persons operating organised market places (OMPs), transparency platforms and platforms for the publication of Inside Information (as defined under REMIT) fall under the NC's scope? Who are the actors that the term aims at encompassing?

(ii) Should large industrial customers be in the NC scope, considering that article 2(1)(a), article 2(1)(o) or article 2(2) could each represent a gateway? E.g.: the definition of electricity entity refers to the definition of "*electricity undertaking*" in the Directive 2019/944 which itself refers to the definition of "*demand response*", hence including final customers participating in demand response. If industrial customers fall in the NC scope, we wonder whether the NC duly takes into account their specificities when defining processes and requirements to ensure an effective NC implementation.

(iii) Electric vehicle charging points: from the current NC wording, it is unclear whether operators of charging points would fall under the NC scope. Considering their potential impact and what seems to be a move towards their inclusion in the scope of NIS2 Directive, we believe it is key for the NC to clarify its applicability to this category of actors.

(iv) The NC should not establish that "*this Regulation shall not apply to a micro or small enterprise ...*" since SMEs are required by this very regulation to comply with the hygiene requirements. They could furthermore be reclassified as high or critical impact entity.

(v) In article 2(2), it is not realistic that any entity listed in article 2(1) can ask for the application or reclassification of other entities or SMEs. It also seems very unlikely that the European Commission would namely ask a person to fall under the NC scope. Finally, point (c) is not applicable as it is not specifying who can re-classify the SMEs or other entities. Is there a link with the current article 27 on the identification of high-impact and critical impact entities?

(vi) The FG mentions that "*the network code could also apply to any other additional stakeholder not listed in Table 1, but with relevant cybersecurity impact on the cross border electricity flow*". In article 2(2) and 2(3), the draft NC refers to "*other entity not listed in article 2(1)*" without any further specifications nor reference to the electricity sector. Therefore, could it involve any actors from any sectors?

(vii) Most cybersecurity operation centres (CSOC) and computer security incident response teams (CSIRT) do not have a legal personality of their own and could not be as such addressees of the NC. In most cases, CSOCs and CSIRT would be created by entities who have a legal personality such as companies or cybersecurity national competent authorities (CS-NCAs).

(viii) We understood from the FG that there will be in practice three categories of entities: (a) the SMEs, (b) the high-impact entities and (c) the critical-impact entities. The category of high-impact entities is meant to include any entities falling under the scope of the NC that do not belong to the categories (a) and (c). We may understand from article 2, and it

has been presented as such during the first ENTSO-E workshop, that there will be in fact four categories of entities: (a) the SMEs, (b) the high-risk entities, (c) the critical risk entities and (d) the other entities falling under the scope of the NC that do not belong to the first three categories and will be subject to the basic hygiene requirements. This is a critical element of the definition of the scope and requirements of this regulation.

By extending the scope of the entities who are only subject to hygiene requirements, the draft NC diminishes the ambition of an increased cybersecurity level across the whole electricity system. While this might be acceptable if this fourth category of electricity entities is small, there would be a significant risk if it were to encompass an important number of electricity entities, leaving only a small set of actors to qualify as high-impact or critical-impact entities and to comply with the associated obligations.

Our recommendation would be to make sure that there are only three categories of electricity entities kept in the NC cybersecurity or, at the very least if the 4th category is kept, that the electricity cybersecurity impact index (ECII) is defined in such a way as to keep the scope of the 4th category limited.

At this stage, it's worth drawing the attention to **article 27(1)** which requires each CS-NCA to identify the high-impact and critical-impact entities in its Member State and allow it to also identify additional entities "*even where they do not individually meet the ECII level*, due to Member State specific circumstances, having regard for the aggregated impact of multiple similar entities on cross border electricity flows." It should be clarified that the SMEs could be part of the "*additional entities*" which can be classified as high-impact or critical impact entity. We also note that the requirement in article 27(1) is very broadly formulated and seems to allow the CS-NCA to identify additional entities without having to comply with a process or having to satisfy any clearly identified criteria. A clear, objective and reliable process needs to be established instead. As solution to be explored would be to ask the CS-NCA to classify the electricity entities in light of the ECII and to make sure that the ECII contains all the sufficient criteria to take into account, for instance, the cases of aggregated impact of a coordinated cyberattack against SMEs.

With regard to the NC objectives, we also have two questions relating to article 3(2) which sets obligations on Member States, competent authorities and regulatory authorities, TSOs and DSOs:

(i) Indent (d) creates an obligation to consult with stakeholders and take into account potential impacts on their systems. What are the systems referred to? For instance, what is the system of an aggregator or a NEMO?

(ii) Indent (e) seems to acknowledge only "*Union standards*" at the detriment of other international standards. This seems inconsistent with article 32(1) and article 49(6) that both refer to international standards for the cybersecurity system and cybersecurity risk management. This is also inconsistent with the existing European practices regarding standardisation. In this regards, we believe that any of the standards satisfying the following conditions should be deemed acceptable: (i) be published by an **International or**

European Standard Development Organisation and (ii) be elaborated under a "*de jure*" consensus process[1]?

3. Governance

Though we have seen significant progress in the definition of the governance in the version of the NC subject to public consultation compared to earlier versions of the NC, we believe that significant improvement still needs to be accomplished especially to satisfy the objective of the FG to reuse as much as possible the already existing governance framework. Our below comments therefore pertain principally to (i) the regime applicable for the elaboration and adoption of methodologies, (ii) the cybersecurity risk working group and stakeholders involvement and (iii) the cybersecurity risk monitoring body. We believe that taking our comments into account would lead to a greater alignment with the existing governance, better understanding for stakeholders and could lead to a streamlined structure of the NC.

The title II could indeed be deleted if, as recommended,

(i) article 15 was deleted and replaced by an article on the creation of a European Stakeholder Committee (as per article 7);
(ii) article 16 was deleted and replaced by an obligation for ACER to consult regulatory authorities in article 5 and monitoring tasks transferred into article 12;
(iii) article 18 was deleted and its risk assessment timings inserted directly in the articles on risk assessment and
(iv) article 17 was grouped together with the other articles on risk assessment.

3.1. Adoption of methodologies (article 5)

We welcome the introduction of article 5 which establishes a procedure for the adoption quite similar to the one found in other NC such as the Regulation 2017/1485 (SOGL). However, some elements still need to be further clarified or completed:

(i) Article 5 refers in some places to the "*competent regulatory authority*" as if a single regulatory authority could be in charge of the adoption of one of the methodology. As article 5 only considers the adoption of Union methodologies by ACER and one regional methodology by all competent regulatory authority of the region, there is no room for the approval by a single regulatory authority and the occurrences of "*the competent regulatory authority*" should be deleted. Likewise, a consistent use of the term "*competent regulatory authorities*" or "*regulatory authorities*" must be ensured. Since contrasting with other NCs,

[1] A *de jure* standard is a technology, method or product that has been officially endorsed for a given application. *De jure* standards contrast with *de facto* standards, which gain prominence through widespread use rather than official endorsement.

this NC vests obligations not only on the NRAs but also on CS-NCAs and RP NCAs, we would recommend to clarify in the Art 5 who the "*competent regulatory authorities*" are. Based on the previous NCs, we would expect those "*competent authorities*" to be NRAs, but the definition of "competent authorities for cybersecurity or CS-NCAs" (article 4(3)) and "*competent authorities for risk preparedness or RP NCAs*" (article 4(5)) instil some confusion which needs to be clarified. It should also be clear for the readers that ENISA does not fall in the scope of the definition of "*competent regulatory authorities*".

(ii) In addition to the methodologies currently listed in article 5(4), we deem it necessary to ensure that there is also an ACER regulatory approval of at least the following methodologies:

(a) The **electricity cybersecurity impact indexes and high-impact and critical-impact thresholds** (article 19(3)(c)) or at least the **rules for the definition of such index and thresholds** (article 17(2)(d)). Given their importance in determining who falls in the NC scope of application and qualifies as high impact entity or critical impact entity, those should be subject to regulatory approval. The rules for the definition of the index and thresholds should be a stand-alone methodology and not only one element of the risk assessment methodology;
(b) The **list of Union-wide high-impact and critical-impact processes** (article 19(2)(a)). Given its importance in the definition of the cybersecurity perimeters and in the performance of the risk assessments, it should not be solely developed in a report and subject to opinion by ACER (article 19(4)) but be subject to regulatory approval;
(c) the **risk impact matrix** that entities and CS-NCAs must use to report the risk identified in their risk assessments (article 19(2)(b)). Given its importance in the performance of the risk assessments, the risk treatments plans and subsequent reporting, it should not be solely developed in a report and subject to opinion by ACER (article 19(4)) but be subject to regulatory approval; and
(d) other elements currently listed in the risk assessment methodology of article 17(2) but which should be stand-alone methodologies.

We also believe that the following "*transitional*" deliverables should be subject to regulatory approvals:

(a) transitional electricity cybersecurity impact index pursuant to article 49(1) ;
(b) consolidated transitional list of high impact and critical impact entities pursuant to article 49(3);
(c) transitional list of high-impact and critical-impact processes pursuant to article 49(4); and
(d) development the transitional list of international standards and controls pursuant to article 49 (5).

3.2. Cybersecurity risk working group (article 15) and stakeholders involvement (article 7)

The creation and the role of the "*cybersecurity risk working group*" is a critical point considering the highly critical and sensitive topics that the working group would be involved with (determining cybersecurity perimeters, indexes to classify high-impact and critical-impact entities, defining metrics and thresholds, etc.). During the first workshop organised by ENTSO-E, it seemed that the drafting team sees itself as a precursor of the working group, somehow shapes its future role and sees the working group not only in support of ENTSO-E and the EU-DSO Entity but as a decision maker.

We however plead for a deletion of article 15 and an amendment of article 7 as we see:

(i) **no need to create such a working group and to list the scope of its tasks**. The responsibility to produce the different NC deliverables is set directly on ENTSO-E and the EU-DSO entity and not on a working group. ENTSO-E and the EU-DSO entity can seek the support of any expert during the elaboration and implementation of the NC and of its methodologies. There is no need to foresee the creation of a working group.

(ii) a sufficient and satisfactory alternative in an **increased stakeholders' involvement.** Beyond the obligation to organise public consultation (article 8), the stakeholder involvement could be reinforced by aligning further article 7 with article 10 of SOGL. This would ensure consistency across network codes and would allow to reuse the structure of the Electricity Stakeholders Committees (ESC) for which ENTSO-E is already providing the Secretariat. We understand that the System Operation ESC created by application of the SOGL is already used to provide updates on the drafting of the NC on cybersecurity. Its scope could simply be slightly extended to also cover the implementation of the code.

3.3. Cybersecurity risk monitoring body (article 16)

We do not understand the role of the "*monitoring body*" whose creation seems to have been proposed only to facilitate ACER's coordination with the other regulatory authorities. It must be noted in any case that this "*monitoring body*" would not be vested with legal personality and would thus at best be an "*advisory board*" or a "*working group*" on whom no obligation could be vested.

Apart from article 16, this monitoring body is only mentioned once in article 7 on stakeholder involvement. If article 7 is further aligned on article 10 of SOGL, it will already allow the coordination with other involved parties.

We believe that it is better to let ACER organise its consultation with the other regulatory authorities rather than impose the format of the "*monitoring bodies*" whose lack of details in the draft NC raises more questions than it answers. We would hence recommend to skip the creation of the "*monitoring body*". At best, an obligation could be inserted in Article 5 to specify that ACER

must consult with the relevant public authorities before adopting a decision on the proposed methodologies.

We also seize this opportunity to highlight our regret that article 12 is currently limited to what seems to be an "*adequacy monitoring*". We would recommend that its scope be extended to the monitoring of the implementation of the NC (not only on the application of cybersecurity Standards) as well as the monitoring of the adoption of the methodologies (items mentioned in article 16). Article 12(2)(c) should also replace the use of the term "size cap" which is not defined or used anywhere else in the NC and article 12(3) should clarify that it refers to articles 30(5) and 32(1) Regulation 2019/943.

4. Cybersecurity risk assessment

The performance of the cybersecurity risk assessment is one of the key pillars of the proposed NC which proposes an article on the establishment of a risk assessment methodology (article 17), but also a risk assessment at Union level (article 19), at regional level (article 20), at Member State level (article 26) and at entity level (article 29). Considering the close links between those articles, we invite to bring them together under the same heading and to use the opportunity to harmonise the chosen terminology ("*risk assessment*" or "*risk management*").

Before sharing our detailed comments and recommendations on those articles related to the cybersecurity risk assessments, we would like to draw the attention to two overarching concerns related to article 18 which defines the cybersecurity risk assessment cycle as taking place on a two years basis:

(i) **Clarity:** several clarifications are required:

a. The transitional regime in article 49 does not contain an end date. We understand that the transitional period will stop when the first risk assessment cycle will start. We thus understand from article 18 that the transition phase may end 18 months after entry into force of the NC. This should be further specified in article 49.

b. The timeline for when the different risk assessments are meant to take place should also be clarified: in the current drafting, one could interpret that all risk assessment are meant to be performed at the same time. It would be better to specify for each article requiring a risk assessment when the obligation should apply. This would allow to then delete article 18 all-together.

c. This would also be an opportunity to clarify the interplay between all those risk assessments and their corresponding deliverables, as it is not clear for the time being how the deliverable of one risk assessment needs to feed into a risk assessment at a different level. E.g.1: clarify that the Member State risk assessment is performed on the basis of the classification of the electricity entities as high-impact or critical-

impact entities made in the previous risk assessment cycle. E.g. 2: clarify when the CS-NCAs is meant to classify the different entities by virtue of Art 27.

(ii) **Feasibility**: within the two years of the risk assessment cycle, many events need to take place: (i) definition of who is a high impact or critical impact entity, (ii) definition of the minimum and advanced controls, (iii) possibility to obtain a derogation; (iv) obligation to comply with the controls and v) obligation to demonstrate compliance with these controls. This comes in addition to the obligations to perform the risk assessments, participate to two cybersecurity exercises on a three-year basis, implement plans for the update of legacy systems, etc. Apart from the multiplicity of obligations, the apparently conflicting timelines lead to a situation where it cannot be easily determined at any point in time (i) who the NC addressees are and (ii) what their actual obligations are. The implementation and compliance with the NC becomes therefore impossible and the objective of the NC to reinforce the cybersecurity of the entire system will be missed. The duration of the risk assessment cycle therefore needs to be lengthened towards a more suitable and realistic timeframe. Alternatively, the four-level risk assessment process (including the deliverables and the interactions between all levels) could be simplified to gain time and therefore allow a rapid adaptation to the always evolving cyber risks.

4.1. Cybersecurity risk assessment methodologies

We consider that the proposed risk assessment methodologies are too vague. Without requiring all the details of the risk assessment methodologies to be provided in the NC, we believe that the NC could already provide more substantial information on the intended content of the risk assessment methodology and of specificities which would apply depending of the geographical level (Union, regional, national or entity level) of the risk assessment.

We furthermore believe that:

(i) The proposed risk assessment methodology should be split into several methodologies. For instance, the rules for the definition of the ECII and thresholds should be a stand-alone methodology considering their importance for the definition of the scope of application of the NC;

(ii) Clarification should be brought on whether the reference in article 17(2) to the "*risk assessment methodologies*" in the plural form means that several methodologies are expected. Would that be one methodology per geographical level? It would mean that we would have several list of threats, several rules for the definition of the index and thresholds, etc.

(iii) The interplay between the different risk assessments at the different geographical levels and their sequence in time, but also the interplay with the reports and other deliverables needs to be clarified.

4.2. Union and regional wide cybersecurity risk assessment

We consider that the proposed approach whereby risk assessments are performed at four levels would lead to a clear view of the state of cybersecurity at the different levels. This would be a very thorough approach. We nevertheless fear that this might be too complex and resource intensive. As a first step to streamline the process while maintaining the benefits, we would recommend to consider merging the Union and regional risk assessments. Their input and deliverables, the methodology and the actors involved are much the same and this may lead to clear synergies and gains in efficiency.

We also have the following comments:

(i) Article 19(2)(a), and throughout the NC: why do we specify "*union wide*" processes since "*high impact and critical impact processes*" are those that already have a cross-border impact? Do we have to consider that it is a new notion or a subset of the notion of "*high impact and critical impact processes*"?

(ii) Article 19(2)(b) : the definition of the "*risk impact matrix*" could have been in article 17 on risk assessment methodologies as it seems to be an element which will be used by electricity entities when making their risk assessment and reporting on it. It is not clear why it is not among the risk assessment methodologies. It is also not clear how this matrix will be used: for the identification and assessments of cybersecurity risks or only to "*report the cybersecurity risk identified*"?

(iii) The list of high-impact and critical-impact processes (article 19(2)(a)) and the risk impact matrix (RIM) should be methodologies subject to consultation and regulatory approval by ACER in accordance with article 5. See point 3.1 of this note for more details.

(iv) Article 19(3)(b): it is not clear what are the "*types*" of entities which could be referred to.

(v) Article 20(2): this paragraph should clarify what information is expected to be integrated and how the integration would take place.

(vi) Article 21(2)(b): it is not clear what are the kind of measures which Regional Coordination Center (RCC) might have to apply in their system operation region. Could that translate in the RCC imposing security controls to the electricity entities at regional level?

(vii) Article 21(4): When are the different regional risk assessments to be performed? Are they synchronized? How do their updates feed into the common cybersecurity framework?

(viii) Article 22: Further clarifications should be provided on the relationship of the cross-border cybersecurity risk assessment with:

a. the Union wide risk assessment report, which actually seems not to be entirely a report and to contain two deliverables which will be necessary for the implementation of the NC. The cross-border cybersecurity risk assessment report on the other hand seems to really be a report aiming at informing its reader.

b. the regional risk assessment. No link is made in the NC despite the fact that it is mentioned in the supporting document. It seems that the report is supposed to be the output of the regional risk assessment.

(ix) Article 22(2)(b): what are "*high level assets*"? How are they identified and defined?

(x) Article 22(2)(g): should we read "*insufficient supply chain security management*"?

(xi) Article 22(2), two-last paragraphs: Though we welcome the participation of all those entities, the way that the obligation is drafted is not clear and not realistic: it is not possible for thousands of persons to contribute to the development of a report. If the goal is to collect data from these entities, it would be better to insert in the NC an article giving the right to ENTSO-E to ask for data to those stakeholders. It would nevertheless raise the question of how this report builds upon the reports coming from the entity level, the national and the regional risk assessments. Isn't the information collected from those assessments sufficient?

(xii) Article 22(4): this article would be clearer if rewritten with first the ENTSO-E and EU-DSO entity having an obligation to create a sanitised version, then this version is to be approved, then it can be published. Finally a sentence can be inserted to explain in which case and to whom a non-sanitised version can be disclosed on a need to know basis.

4.3. Risk assessment at Member State level

Concerning article 26, we do not understand the meaning of article 26(2)(a) and propose the following reformulation: " *the ~~overall~~ likelihood and consequence* ***of risks in its Member State that can impact on high-impact and critical-impact processes at Union level ; these risks should be assessed according to*** *~~on~~ the risk impact matrix* ***defined in Article 19 (2)(b).*** *~~of a successful cyber-attack compromising the Union-wide high-impact and critical-impact business process in its Member State~~".* In article 26(2)(b), we wonder why the threats and vulnerabilities should be limited only to those contributing to this "*likelihood*".

4.4. Risk assessment at entity level

As a preliminary comment, it seems apparent that, when reading the draft NC, the different parts of the draft have been elaborated in parallel and that further consistency and coherency could be ensured between those parts. With regard to the risk management at entity level, **article 29** proposes to bring together in a single article all aspects related to context establishment, cybersecurity risk assessment, risk treatment and risk acceptance. Those aspects have been treated in different, autonomous articles respectively for the Union, regional and national level. The reason justifying such a difference of approach (integrated approach vs. split up approach) is not clear. In this respect, we would recommend to maintain the parallelism of the articles between the Union, regional, national and entity levels.

The interplay of the risk management at entity level with the risk assessments and their deliverables at Union, regional and national levels is not apparent in the draft NC:

(i) How does it integrate within the two years risk assessment cycle?

(ii) Is the "*scope of the cybersecurity risk assessment*" (article 29 (3)(a)) the same as the cybersecurity perimeter?

(iii) Should the "*criteria for risk evaluation and for risk acceptance*" (article 29(3)(b)) simply be "*in line*" or actually be the same as the risk impact matrix (article 19(2)(b)?

(iv) Why must the list of threats of Art 22(2)(c) only be "*taken into account*" (article 29(4)(ii)) and not reused as is?

(v) Why is there a specific obligation to identify risks by taking into account vulnerabilities including those caused by legacy system (article 29(4)(iii)) when this seems to already be a requirement from the risk assessment methodology (article 17(2)(e))?

(vi) What justifies the divergence in the description of the possible cybersecurity incident scenarios (article 29(4)(iv)) from the description which is given of the "*consequences of cyberattacks*" in the other articles relating to risk assessments at Union, regional and national levels?

(vii) Are the provision of article 29(4)(c) inconsistent with those of article 29(1) that mentions that the cybersecurity risk management is applied to "*all assets in its high-impact and critical-impact perimeters*"? This assumes that the high-impact and critical-impact perimeters are already known.

(viii) In article 29(5), electricity entities have to report the controls that they implement for risk treatment to its NRA and its CS-NCA. It would be meaningful only if the electricity entities also have to share the results of their risk assessment and/or their whole risk treatment plan with its NRA and its CS-NCA. Otherwise, the NRA/CS-NCA won't have a global picture allowing it to identify all the vulnerabilities and especially those for which there is no control implemented.

(ix) Who defines the acceptance criteria mentioned in article 29(6)? This article would need to be developed further and explain clearly that two different services within the entity are designing the treatment plan and accepting it

(x) Article 29(7) refers to the assets identified in paragraph (2). However this paragraph does not mention assets.

With regard to article 29(3)(a), we understand that the scope of the cybersecurity risk assessment is to be defined in relation to the high impact and critical impact processes identified in the report of the pan-EU risk assessment in article 19(2)(a). The exact interplay between those two is nevertheless unclear and should be clarified if we want to ensure a coherent and harmonised implementation of the NC across the EU and therefore an increased level of cybersecurity in the EU.

Finally, it must be noted that, as the scope of the cybersecurity risk assessment for the electricity entities is to be defined in relation to another deliverable of the NC which is out of their controls, it is impossible for electricity entities to know in advance the exact scope of their cybersecurity perimeter and what efforts they would have to make to comply with their obligations stemming from the NC.

On article 31(1)(b), we do not understand the reference to the notion of "*confidentiality, integrity and availability*" of the high-impact and critical-impact processes that does not seems to be defined. Couldn't we simplify by mentioning "*the compromise of the high-impact and critical-impact processes*"?

In **article 32** on the Cybersecurity management system, the description at high level of the cybersecurity management system is welcomed. It brings a certain level of harmonisation and it leaves a margin of discretion for the electricity entities to organise as they see fit even though critical impact entities would nonetheless have to verify the compliance of their cybersecurity management system in accordance with the framework established under Art 33.

We nevertheless believe that a series of points have to be clarified:

(i) Who are "*the parties affected by the security risks*"?
(ii) How can one demonstrate the "*leadership and commitment*" of the top management? Who is the "*top management*"?
(iii) What are the resources which are referred to in point (c)? Human resources? Financial resources? Are we speaking of the same resources in point (g)?
(iv) What are the "*roles*" which are referred to in point (e)?

5. Common electricity cybersecurity framework

Title IV of the draft NC provides for the establishment of the common electricity cybersecurity framework. To form a coherent part, we believe that the provisions of additional articles related to the common electricity cybersecurity framework should be brought together under this title: article 30 on derogations from the minimum and advanced cybersecurity controls, article 32 on the cybersecurity management system and article 33 on the verification of the common electricity cybersecurity framework. It might call to change the name of Title IV to reflect more accurately its scope.

5.1. General comments

In its current shape, the common cybersecurity framework is neither clear nor sufficient to achieve the objectives of the NC. It is not even clear when the first common electricity cybersecurity framework should be elaborated: this needs to be clarified if one does not want to see this obligation apply as from the NC's entry into force. Article 23(1)(a) should also be amended to apply to both the high-impact and the critical-impact perimeters and not only to high-impact perimeter.

More generally, questions arise with regard to (a) minimum and advanced cybersecurity controls and (b) the mapping to standards and national legislations.

(a) Minimum and advanced cybersecurity controls

When reading article 23 in isolation, one understands that there is no indication on how the minimum and advanced cybersecurity controls of the common cybersecurity framework will be defined. It seems to give a blank check for ENTSO-E and the EU DSO Entity to define the security controls as they wish. It begs the question of the definition of those minimum and advanced controls and we believe that more information should be provided in the NC as to the key elements composing those controls. At the very least the objectives that those minimum and advanced controls aim at reaching should be explicitly stated in the body of the NC to provide sufficient indications to the electricity entities.

We however and furthermore understand that the intent for the minimum and advanced controls referred to in article 23 is to be composed of two subsets:

(i) The "*regional*" minimum and advanced controls, defined in accordance with article 21 as a result of the of the regional cybersecurity risk treatment plan;
(ii) The "*supply chain*" minimum and advanced controls, defined in accordance with article 24 and for which a list of five requirements is already listed in article 24(2).

In this regard, we identify two major inconsistencies with the current draft which need to be addressed:

(i) Even though the "*regional*" minimum and advanced controls would result from a regional assessment, they are intended to be harmonised for the whole of the Union. This can be seen in the fact that those controls are meant to be integrated in the common framework approved by ACER and this approach was confirmed by the drafting team.
(ii) Three different types of regulatory approvals are foreseen for the minimum and advanced controls: a) by the regulatory authorities of the system operation region for the "*regional*" controls (articles 5(5) and 21), b) by ACER for all controls once integrated within the common framework (articles 5(4) and 23) and c) by no one for the "*supply chain*" controls (until they are integrated in the common framework) (articles 5(4), 23 and 24).

As the minimum and advanced controls could have a significant impact on the obligations of the electricity entities, it is important to have a single, clear and efficient set of controls and regulatory approval.

(b) the mapping to standards and national legislations

The common framework also lacks clarity on (i) how the standards and national legislation will be mapped, and (ii) whether ENTSO-E and EU DSO entity can exercise any discretionary powers to accept the mapping with those national legislation.

We furthermore identified two issues since, when evaluating the equivalence of the national legislation, the "*conformity assessment body*":

(i) might not be in a position to evaluate the work of the public authorities/CS-NCA/NRAs; and
(ii) should not be asked to evaluate whether the national legislation is "*sufficiently equivalent*" but "*equivalent*": we should be sure of the equivalence and not be satisfied with similarities.

It also seems that the transitional common framework, which must be established really quickly after the entry into force of the NC, might lead to excluding some of the national frameworks. Some national authorities might not be in a position to demonstrate in time the equivalence of their national legislation in the transitional common electricity cybersecurity framework. This might create a precedent and disincentivises national authorities to seek the inclusion of their national legislation in the long lasting common electricity cybersecurity framework. This might also disincentivise electricity entities from relying on the expected equivalence of their national legislation.

5.2. Cybersecurity hygiene requirements

Article 2(2) mentions that the basic cybersecurity hygiene requirements as defined in Annexe A shall be implemented by SMEs and any other entity not listed in article 2(1) within 12 months after the entry into force of the NC.

We welcome the idea of basic requirements applying to all electricity entities: it ensures that all actors are involved in the cybersecurity of the system, with obligations proportionate to their potential impact on the system. However, we wonder whether the requirements are not too vague. More detailed and refined requirements could usefully be developed, based on the detailed work of the ENISA in its "*Review of Cyber Hygiene practices*". In this regard, some CS-NCA have already published detailed national guidelines on cyber Hygiene good practices directly derived from the ENISA recommendations and the implementation of these good practices are still in progress within the concerned actors.

This development could be done directly in the Annex A or in a subsequent methodology whose elaboration would have to be mandated in the NC and which would be submitted to regulatory approval. In that case, the impact of those reinforced requirements on the cybersecurity of cross-border electricity flows would be reinforced and the time for their implementation might have to be slightly extended.

We would like to draw your attention on the fact that these hygiene requirements are currently planned to be applied by SMEs without clarification of the scope of their application, i.e. without stating the relevant assets perimeter. As it would be too burdensome to determine the assets perimeter through a risk based approach, we would recommend instead to provide in the draft

NC that the hygiene requirements apply only to the IT and OT processes, services and tools which are directly used for the performance of the core operational activities of the electricity entities (e.g.: for the activities of generation for a generator, but not for an HR management software for instance).

The "*12 months*" delay granted to comply with this cybersecurity hygiene requirements might need to be extended if the hygiene requirements were to be deemed applicable to all assets without a limitation to the assets linked to the core operational activities of the companies.

5.3. Standards mapping matrix

We are not sure to understand the added value of article 25. Does not article 25(1) says the same as Art 23(1)(c)? Shouldn't the two paragraphs be merged?

Article 25(2) provides that "*If the CS-NCA and NRA provide a mapping, they shall have a conformity assessment body verify that the national requirements are sufficiently equivalent to the minimum and advanced cybersecurity controls*." We have a few comments regarding this sentence:

(i) Shouldn't the elements of this paragraph be part of Art 23(1)(c)?
(ii) Shouldn't it be "CS-NCA or NRA"?
(iii) Why "*sufficiently*" equivalent? Is there any other alternatives of being equivalent or not?

5.4. National verification schemes

For the implementation of article 28 on the national verification schemes, we wonder whether competitors in the electricity sector would be in a situation of "conflict of interest" as meant in article 28(2)(a) and whether they would therefore be in a position to be performing "*peer review*" for one another. The notion of "*peer review*" should be further defined in this article or in article 4.

5.5. Derogations

With regard to the process followed for granting derogations in **article 30**, we recommend several modifications to streamline and increase the robustness and efficiency of the process:

(i) There should be only one entity in charge of granting the derogation: the responsibility is currently vested with two public authority which raises questions of efficiency and of conflict resolution in case those authorities reach diverging decisions to grant or not derogations;
(ii) A deadline for granting the derogation should be inserted in article 30, so that both the requester and the public authority can rely on an expected timeline;

(iii) The process needs to be streamlined so that electricity entities can quickly benefit from derogations and can then focus their efforts on complying with their obligations. For the time being, we understand that a derogation would be granted at best in the 21st month of the 24 months risk assessment cycle, which would leave only 3 months to ensure the compliance before the start of the next risk assessment cycle.

With regard to the conditions listed for the derogation (article 30(2)), we believe that they need to be further worked upon to ensure their legal robustness and make sure that the view of the electricity entities plays a proportionate part in the assessment of the derogation requests:

(i) On condition (a): against which objective criteria do we evaluate that the costs exceed the benefits? And what if the costs are very important but that there is still a great benefit for the entire system? Are the benefits to be assessed for the electricity entity or for the system?
(ii) On condition (b): the risk acceptance criteria is defined by the electricity entity: the electricity entity should not be in a position to be "*judge and party*". There needs to be an external assessment by a public authority.
(iii) On condition (c): by definition, the obligations for which a derogation is sought are applying to high impact or critical impact entities (minimum and advanced cybersecurity controls), which means that those entities are deemed to have a cross-border impact. How could a risk assessment therefore demonstrate that there is no impact cross border?

Concerning article 30(3), we wonder whether the derogation granted "*for a maximum of two year*" could be renewed. We also do not understand who will be the "*entities*" to be consulted.

5.6. Verifications and inspections

In article 33, it is currently proposed to apply the obligation to verify the conformity with the requirements of the management system and of the minimum and advanced cybersecurity controls solely to the critical entities. We believe that this should be extended to the high-impact entities to ensure their compliance and conformity with their obligations. The title of article 33 should be modified as it is not about "*verification of the cybersecurity Framework*", but about "*verifications of (High &) Critical Entities*".

Regarding the cybersecurity inspections, we recommend to clarify in article 34 what the notion of "*joint inspection*" means under paragraph (a) and what the difference between paragraphs (a) and (c) is.

6. The Supply chain security control (article 24) and procurement requirements (articles 35 & 36)

As a general comment, we believe that the NC should set obligations directly on the suppliers providing goods or services to electricity entities. This would ensure that the supplier is committed to the cybersecurity dimension of the products and services it supplies and, consequently in the cybersecurity and operational security of the electricity system as a whole. In the absence of such an obligation, we fear that there would be no level playing field between suppliers and the electricity entity, the former being potentially more inclined to push back against the procurement requirements that the electricity entity would like to impose. The obligation would move the topic of cybersecurity from an issue of contractual negotiations between parties of different strengths to an issue of compliance of the parties with their legal and regulatory obligations.

As regard the articles, the wording of **article 24** is to be improved to precise the scope of the obligations with regard to the supply chain. Among others, the use of the term "*appropriate*" to refer to the "*appropriate level of suppliers' cybersecurity risk-level*" and "*appropriate depth and coverage of the verification*" should be clarified. It is not clear what would be deemed "*appropriate*" or who would make this appreciation?

With regard to the procurement requirements for the supply chain as referred to in article 35(2), we understand that ENTSO-E and the EU DSO entity would develop harmonised cybersecurity procurement requirements in accordance with article 35 and that those would not be made mandatory. We understand that electricity entities would still be allowed to develop their own cybersecurity procurement requirements but that those would have to cover at least the points listed in article 24(2)(a)(i) to (ix). In this regard, we wonder what is the latitude left for electricity entities to define their own cybersecurity procurement requirements and/or what room for manoeuver there is to distinguish between the harmonised cybersecurity procurement requirements of article 35 and the minimum requirements listed in article 24(2)(a)(i) to (ix).

Article 24(3) refers to a "*verification scheme pursuant to article 36*". However, article 36 does not put in place a verification scheme but only a possibility for the ENTSO-E to establish a guidance to help electricity entities determine if a priori their procurement is compliant. Therefore it is not correct to mention at article 24(3) the possibility to verify through article 36. Neither is it clear what the other "*verification activities*" referred to here are.

As regard Title VII on harmonised cybersecurity procurement requirements, our understanding is that the goal of both articles 35 and 36 is to explain that ENTSO-E and the EU DSO Entity have the right and possibility (though no obligation) to develop: (i) non-binding CS procurement requirements as well as (ii) Guidance on the Union certification schemes. Therefore, none of the articles are meant to create real obligations.

For article 35, wouldn't it be better to explain in one sentence in article 24 that ENTSO-E, in cooperation with the EU DSO entity, shall have the right to develop a non-binding harmonised cybersecurity procurement set of requirements respecting the parameters of article 24(2)(a)? If doing so, ENTSO-E would have to (a) ensure that the set of cybersecurity procurement requirement is compatible with Union certification schemes and (b) consult stakeholders in accordance with article 8 and take into account the comments.

For article 36, wouldn't it be better to explain in one sentence, still in article 24, that ENTSO-E, in cooperation with the EU DSO entity, shall have the right to develop a non-binding guidance on the Union verification schemes that help critical-impact entities to determine whether an ICT product, ICT service or ICT process meets the harmonised cybersecurity procurement requirements. When doing so, ENTSO-E would have to (i) cooperate with ENISA and (ii) consult stakeholders.

Actually, on article 36, we do not see any role for the ENISA in designing or approving the guidance. Wouldn't it be better for ENISA to be the author of such guidance, with the support of ENTSO-E and the EU DSO Entity for its elaboration?

If those recommendations are followed, this Title VII could be deleted.

If article 35 remains, a timing must be inserted in the article for the first adoption of the work programme and, if need be, for its subsequent updates. Without timing, the obligation has to be complied with as from the first day of application of the NC.

7. Essential information flows, incident and crisis management

As a preliminary comment, we support the principle enshrined in **article 37** to ensure that the CS-NCAs and CSIRTs share information with the relevant electricity entities to allow them to enhance their defence. We nevertheless would like to share some practical considerations which we believe need to be taken into account so that this article and the sharing of information which it supports can effectively be implemented:

(i) A lot of exchange and sharing of information needs to take place between CSIRTs and with high and critical entities, among others in relation with close to real time data coming from across Europe. It does not seem opportune or realistic to have such a level of ambition and to proceed to such exchange and sharing of information "*manually*". An IT tool supporting the process is therefore recommended.

(ii) In light of the above, article 37(8) should be redrafted so that it does not only merely foresee a feasibility study for the development of an IT tool but rather (a) clearly plan for the development of such a tool; (b) allocate the responsibility to such a tool on an actor, (c) determine key requirements in terms or availability, redundancy, resilience, back-up,

functionality and cybersecurity of the tool itself and (d) allocate sufficient funding for such a tool.

(iii) Throughout article 37, there should be clearer indications in terms of timing: (a) when does the clock starts ticking when information needs to be submitted within x hours?; (b) should the CSIRT and CS-NCAs be available 24/24 and 7/7?; (c) do we speak of business or calendar days, of business or regular hours? Those are key dimensioning parameters which need to be clarified so that the cybersecurity of the electricity system can be effectively ensured at any given point in time throughout the year and the relevant investment may be made to comply with the NC obligations.

(iv) In terms of applicability, it should also be clarified when the IT tool needs to be made available and when the obligations relying on the availability of such a tool should start applying. It does not seem appropriate to ask CSIRTs to comply with those obligations if they are not realistically given the means to comply with those. Similarly, it seems important to clarify what should happen before its commissioning date and in case the IT tools becomes unavailable.

The same series of comments and questions arise with regard to the Electricity Cybersecurity Early Warning Capabilities (ECEWC) which we understand can function only on the basis of a developed IT tool. The draft NC should also clarify the obligations of all actors when using the ECEWC to ensure a smooth flow of information.

As CSIRTs are concerned, we would also want to seize the opportunity to draw the attention to the proposed definition of "CSIRT" in article 4. According to this definition, the CSIRT would not only be in charge of the incident handling but would also be responsible for risk handling. We do not support this definition as we do not believe that it is the responsibility of a CSIRT to manage the risk.

Though we appreciate the great efforts which have been put into the elaboration of this title to bring a much-needed common framework to share essential information and address incidents and crisis, we believe that a number of points need further improvement in this title:

(i) The title often refers to "*CSIRTs*" and to "*CSIRTs of the Member State*" whose roles and responsibilities are different. It however seems that the two terms are sometimes used interchangeably: this must be reviewed to ensure that each actor is vested with the appropriate obligations. In a similar manner, article 38 refers to "*MSSP or another entity providing the service"* without the distinction between the two entities being clear. This would have in any case to be consistent with future NIS2 Directive.

(ii) Article 37 allocates obligations on the CS-NCA or CSIRT: it should be clearer on which actor the obligation is allocated. It cannot be allocated to both at the same time or leave it as an alternative. The uncertainty creates a risk that the obligation is not complied with at all.

(iii) Article 37(4) allows the CS-NCA or the CSIRT to assess the level of classification of the information and to inform the entity of the outcome of its assessment: it is not clear against

which parameters this assessment is made or what concrete actions could come out of the assessment. Do the CS-NCA or the CSIRT have the power to reclassify the information without the consent of the originator?

(iv) In article 37(5)(b), who determines the relevant technical information, according to what process and against which criteria ?

(v) What is the goal and purpose of ENISA's guidance on establishing CSOC capabilities (article 37(6)? Would this document become a reference document that electricity entities would be asked to align with? What would happen in case they do not align with it?

(vi) In Art 38(1)(b), it is not clear what the obligation for the electricity entities to "*encourage the provision of automated tools including AI*" for the CSOC capabilities means: who does it need to encourage if not oneself? Should the AI tools really be mandatory?

(vii) Article 38(2) refers to the notion of "*reportable incident*" that is also mentioned in article 37. Should we consider either a cross-reference or the drafting of a definition in article 4?

(viii) In article 38(5), it is explained that the electricity entity must indicate "*the legal basis under which the information is reported*".

A**rticle 39** is mainly creating obligations on the electricity entities. There are mentions of the CS-NCA, the CSIRTs, the CSIRT network, the ENTSO-E, the EU DSO entity, the RCCs and ENISA supporting but it is not clear how their help can be sought nor what kind of help they could provide. Similarly, the CS-NCA or CSIRT of the Member State is meant to coordinate the exchange of information between CSOCs or MSSP of different electricity entities, but it is not clear how. Though we support the intention to provide support, it is not clear how this support could materialise and it is therefore doubtful that any help would actually be provided.

Similarly to article 39, **article 40** foresees that support is to be provided to the electricity entities but it is unclear how such support would actually be provided. It becomes doubtful that it actually would be provided. Among others, it is still unclear how the authorities would provide support, how the ad hoc group would be constituted, or whether it would really be allowed to join the Cyber Crisis Liaison Organisation Network (CyCLONe). Even if the information can indeed be reported up, it is not clear what financial, technical, human resources or tactical resources would be made available to the electricity entities in return.

A**rticle 41** on crisis management plans and business continuity plans requires the elaboration of cybersecurity crisis management plans for the electricity sector by ACER at EU level, by the NRA at Member State level and by electricity entities at entity level. The article fails to explain what should be contained in the first two plans and to establish clear links between all those plans. Article 41(4)(a) also seems to require electricity entities to provide for rules of declaration of a crisis as described in the Risk Preparedness Regulation but it is not clear what is meant exactly as under this Regulation only the competent authority (e.g. government) can declare an electricity crisis.

8. Electricity cybersecurity exercises

We support the approach that consists in running regular cybersecurity exercises alternatively at entity, national and regional or cross-regional levels. We understand that it would in practice lead to exercises to be run at the entity or national level every three years and at the regional or cross-regional level every three years. Combined with all the obligations stemming from the two-year risk assessment cycle, we nevertheless fear that it might represent a very burdensome workload. We also have a series of concerns as to the practical implication of the organisation of those exercises at this stage:

(i) In terms of resourcing (people or technology) and associated efforts
(ii) In terms of finance, and
(iii) In terms of general coordination:

- For the corporate groups operating in different European Member States, a major concern relates to the organisation of Group exercises. We see a very beneficial impact of Group exercises and believe that it would be worth to preserve them. We see that the European cybersecurity exercises could be an opportunity to organise those Group exercises, given that the specificities of a Group functioning are well taken into account. The organisation of cyber exercises at national level might prove more problematic if it is not sufficiently coordinated between the CS-NCAs as it might lead the different CS-NCAs to subject the subsidiaries of a same Group to cybersecurity exercises according to different timings and scenarios. This would not allow to make use of the Group synergies, including but not limited to our Cyber Group Crisis Organisation, and would on the contrary endanger the capabilities of the group's SOC and CSIRTs who would constantly be involved in cybersecurity exercises and not able to focus enough time and resources on their operational activities.
- We note that critical impact entities would be asked to require their critical service suppliers to take part in their cybersecurity exercises. This requirement needs to be written into the contracts with the critical service suppliers prior to the start of the cyber exercises. It must be taken into account that renegotiating those contracts might take time and is not a given as it would create new obligations on the critical service suppliers which they are not likely to agree to without compensation. An obligation to participate in the exercises coming directly from the NC would facilitate the process in this regard. In any case, if this issue is solved, we still wonder how the coordination of a critical impact entity with its suppliers would impact its preparatory work for the cybersecurity exercises, especially in case it has several critical service suppliers or that the critical service suppliers is bound towards several critical impact entities.

Moreover, we understand that a successful cybersecurity exercise will be composed of four consecutive phases post risk identification: (i) definition of the scenarios; (ii) definition of the key success criteria, (iii) running the cybersecurity exercise itself and issuing a lessons learnt report and (iv) compiling an action plan to include some remediation activities. We fear that the draft NC does

not respect those four steps or tend to mix them: the terminology is key here. We note for instance that the article 45(5) foresees a periodic analysis of the lessons learnt and recommendations. The lessons learnt will be "frozen" post exercise. The analysis should be on the action plan and its remediation actions, progresses made etc. It should not lead however to a review of the lessons learnt.

More generally, we believe at this stage that the proposed electricity cybersecurity exercise framework cannot be deemed to be clearly described and be sufficient to meet the objectives of the NC. There are still uncertainties on several points:

(i) Like many other obligations in the NC, the organisation of cybersecurity exercises is dependent on the definition of the critical processes. It is therefore not possible at this stage to have a clear overview of the obligations on the electricity entities in terms of cybersecurity exercises.
(ii) The NC does not specify at this stage in which language the cybersecurity exercises should be organised in. This is something which should be clarified for the regional and cross regional exercises and for each exercise having a cross-border impact (for instance for Group exercises). If a unique language is to be used, this might lead to practical steps to be taken to ensure that sufficient language skills are available within the electricity entities.
(iii) The key success criteria are not defined for the moment in the NC. The absence of a proper definition does not allow to determine the success of the exercise nor of the remedial actions to be adopted to remedy the vulnerabilities.
(iv) It is not clear for the time being in the NC who will produce or contribute to the lessons learnt report, or what would be the governance model for the national or regional cybersecurity exercises.
(v) There is no indication as of yet on the anticipated duration of the cybersecurity exercises. Whether they are meant to last for a day or a week would have a significant impact on the estimation of the costs, resources and capacity management.
(vi) Finally, we believe that it is important to stress that the organisation of all those cybersecurity exercises will require additional funding and that it will have significant financial costs. Is there any mechanism foreseen to support electricity entities face those costs?

9. Confidentiality

9.1. Confidentiality of entities lists

Following their classification by the relevant competent authorities, the NC proposes to establish a list of high impact and critical impact entities. This obligation exists under article 49 (2) and (3) for the transitional list and article 27(2)(a) for the long lasting list. Those lists come from the national levels and are transferred, according to the NC, to ENTSO-E and EU DSO Entity. Article 2(2) also

provides that NRAs and NCAs keep a list of SMEs and other entity that fulfil the condition of article 2(2)(a) and (b).

The draft NC even proposes that the transitional list must be (i) shared with ACER, the Commission, ENISA, the CS-NCAs and the NRAs and (ii) published by ENTSO-E and the EU DSO Entity on their website. The draft NC also requires the Cybersecurity Working Group, which is composed of a great number of actors whose compliance with the confidentiality requirements cannot therefore be ensured, to support the development of the long lasting list of high impact and critical impact entities.

This approach is not acceptable and the lists should be kept as confidential as possible. Falling into the wrong hands, it could constitute the ideal target lists for cyber pirates, thus able to determine the level of protection and therefore the potential vulnerabilities of the electricity entities. We therefore urge for the publication of the entity lists to be removed from the code, for a confidentiality principle to be associated with those lists, for the circulation of the lists to be restricted only to those who need to have access and for additional mechanisms to be put in place to ensure that the communication of such lists take place through cyber secure means thus reducing the risk of leaks. This request is in line with the Framework Guideline that mentions that "*the list will be treated as a sensitive information and manage jointly by the CS-NCA and the NRA, ACER and ENISA*". In this regard, the fact that the long lasting list should be delivered by CS-NCA to the ENTSO-E and EU-DSO entity is questionable if they do not put in place a secure environment for the transfer and retention of these lists (article 27(2)(a)).

A similar reasoning should apply to any list or report potentially highlighting the vulnerabilities of electricity entities. This is particularly the case for instance for the reports required after the risk assessments at regional level (Art 22), national level (Art 26(2)) and entity level (Art 31).

We take the opportunity of these comments on the confidentiality framework of lists to note that the NC explicitly provides that "*the transitional list of high impact and critical impact entities 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*". Such a precautionary principle is however missing with regard to the long lasting list established after the end of the transition period and its subsequent amendments. It would thus theoretically be possible for an electricity entity to move back and forth between the status of critical impact and high impact entity. To avoid such uncertainty, we invite you to ensure that a similar precautionary principle applies to each evolution of the list of entities.

In light of the above, we may understand that the competent authorities have no discretionary power to establish the list of entities when applying the ECII thresholds (which is not clear in the light of the current draft NC), it might be opportune to build the precautionary principle within the

ECII. When determining who qualifies as critical impact or high impact entities, the competent authorities would not run the risk of demoting any electricity entity.

9.2. Confidentiality information (article 10) Information Confidentiality Classification and protection (article 11) and Rules for making and protection of confidential information (article 47)

We believe that ensuring the right protection of information is a key parameter to create an environment where the different actors trust each other and share the necessary, relevant information to prevent, detect and deter cybersecurity threats, incidents and crisis.

We believe that significant improvement is needed to ensure a robust protection of information in the framework of the NC:

(i) Article 46 lists a lot of principles and objectives in view of protection the information which needs to be exchanged in the framework of the NC: principles of transparency, proportionality, accountability and efficiency and objectives of protection from unauthorised access, use, disclosure, modification or destruction, protection of confidentiality, integrity and availability. However, article 46 does not provide any clear indication of what the principles and objectives mean in practice nor on who must comply with them. The article needs to be redrafted so as to establish clearer obligations with clearly identified addressees.

(ii) Article 46 furthermore needs to be enhanced to ensure that it is actionable and provides a clear roadmap to be followed by the actors when handling information. For instance, it should not be for the addressees of the NC to wonder how to ensure their compliance with the already existing other pieces of legislation on data protection (protection of commercially sensitive, confidential information and trade secrets, Regulation (EU) 2016/679 and Regulation (EU) 1227/2011 but the NC should provide a streamlined framework which ensures that there is no conflict with those other pieces of legislation.

(iii) Articles 11, 46, 47 and 48 all require to classify the information. It is not clear whether it relates to the same or different classifications. This needs to be clarified so that stakeholders have only one clear set of obligations to comply with. It seems furthermore that there are inconsistencies in the approach supported, the article 11 focusing for instance on the interests of the information originator whereas article 46 focuses on the interests of the EU and its Member States. The categories used for the classification of the information diverge also between the articles in the NC but also diverge from the classification used in the Commission Decision (EU, Euratom) 2015/444. The coherency and consistency need to be ensured.

(iv) Article 47 only creates an obligation to classify the information in different categories but does not explain what regime applies to those different categories of data. The classification is not sufficient to ensure the application of a legal regime of data protection. This needs to be made more explicit. In the same way, is the possibility for the data originator to "limit distribution, restrict use or indicate releasability" supposed to be binding

and if so, what is the interest of the classification of data in the first place? Are the rules of Chapter 4 of the Commission Decision (EU, Euratom) 2015/444 supposed to apply by analogy?

(v) Articles 47 and 48: it is not clear whether both articles are meant to apply to the information exchanged in the context of Title VIII.

10. Benchmarking

The FG provides in article 8(2) that the NRAs shall carry out a benchmark on investments made by entities in the scope of the NC. This topic is covered by article 13 of the draft NC.

In this regard, NRAs may consider that they are not legitimate to require communication of expenditures from entities that are not regulated (i.e. transmission and distribution operators). Incidentally, we may also consider that NRAs have already all the powers to ask to transmission and distribution operators their cybersecurity expenditure in the frame of the definition of the transmission and distribution tariffs. Therefore should this benchmark covers all entities in the scope of the regulation, it would likely be conducted by the CS-NCA.

Notwithstanding the national authorities that will conduct this benchmark and based on exchanges we had with cybersecurity experts, we wonder whether it will be relevant to make a benchmark based on collection and comparison of cybersecurity expenditures even per activities (e.g. generation, aggregation, supply, distribution, etc.). At this stage we do not see any benefit nor real practical use for this benchmark. It will be in any case difficult to correlate the level of spending with the maturity of the actors and then of the sector and to draw conclusions or recommendations from such results. It may end up in a very burdensome process that will not serve any purpose.

As a stakeholder, we would better support voluntary exchange of best practices between actors of the sector, in the respect of competition law rules.