Response ID ANON-BWFN-QDMZ-9

Submitted to Network Code on Cybersecurity
Submitted on 2021-12-10 15:35:20

Introduction

1 What is your name?

Name:
Andres Pinto-Bello

2 What is your email address?

Email:
andres.pintobello@smarten.eu

3 What is your organisation?

Organisation:
smartEn Smart Energy Europe

4 Privacy Policy

I agree to ENTSO-E's Consultation Hub Privacy Policy (see bottom of page):
Yes

5 Terms of Use

I agree to ENTSO-E's Consultation Hub Terms of Use:
Yes

6 Do I want my answer to remain anonymous?

No, feel free to publish my comments

Title I: GENERAL PROVISIONS

7 Are the objectives of the Network Code on Cybersecurity, which lays down sector-specific rules for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management sufficiently clear?

No

If your answer is "No", please elaborate:

European legislation should strive in creating a pan-European framework that facilitates activity in all Member States, with one of its key roles being, avoiding market fragmentation by having individual MS implementing their own frameworks. For this reason smartEn thinks that the cross-border focus should be expanded to a more holistic one. Even if the NCs are drafted principally to address cross-border issues, we would recommend the objectives to be reviewed to put less emphasis on the cross-border flows of electricity and rather focus on pan-European harmonisation. They should focus on ensuring the cybersecurity of the entire electricty system, from end to end, so as to ensure the operational security not only of the cross-border flows but of the entire system. See for instance the Article 4 System Operation Guidelines (SOGL - Regulation 2017/1485) which does not stress as much on the cross-border impact and focuses on the operational security of the system. To avoid any overlap and conflicts with the NIS 2 Directive, clear alignment is necessary on the responsabilities of each file.

8 The NCCS states: "Notwithstanding any other provision of this Regulation, a micro or small sized enterprise and any other entity not listed in Article 2 (1), not classified as a critical-impact or high-impact entity, shall implement the basic cybersecurity hygiene requirements as defined in Annexe A within 12 months after entry into force of this Regulation." Based on the statement above, are twelve months a reasonable timeframe?

Not Answered

If your answer is "No", please elaborate:

9 The NCCS states: "Notwithstanding any other provision of this Regulation, a micro or small sized enterprise and any other entity not listed in Article 2 (1), not classified as a critical-impact or high-impact entity, shall implement the basic cybersecurity hygiene requirements as defined in Annexe A within 12 months after entry into force of this Regulation." Based on the statement above, do you think these requirements for small and micro enterprises are of sufficient level?

They are too strict

If your answer is "They are too strict" or " They are too flexible, more strict requirements should be in place", please elaborate:

smartEn supports a common set of harmonised minimum requirements for all energy entities, with proportional obligations based on the risk level they suppose and their impact on the system. This includes at the grid edge to ensure trust in prosumer business models by making sure that the electricity system as well as prosumers themselves are protected against cybersecurity risks.
Requriements should be selected from ISO/IEC 27001 with implementation options in ISO/IEC 27002. A proprietary list could lead to variable interpretations and difficulties to find support in the market. Proportional minimum requirements should be rutinely revised, to make sure that no discrimination is possible between SMEs, and other critical-impact or high-impact entities and that there are no significant different levels of protection between IT-systems.

10 Do you consider the Monitoring approach defined at Article 12 to be effective to monitor the adequacy of the Network Code to the ever-changing technology landscape and evolution of applicable cybersecurity standards?

No

If your answer is "No", please elaborate:

smartEn would like to highlight the inconsistencies in the allocation of the responsibilities between ACER and the so called Monitoring Body. Whereas Art 12(2) seems to vest ACER with the sole responsibility to evaluate the adequacy of the NC CS, the Monitoring Body would be vested by Art 16(2) with the responsibility to monitoring the implementation of the NC CS and of its methodologies. To avoid doubling and diluting of responsabilities, we propose that all those activities should be clearly allocated to ACER, in the fremework of the Art 12 on monitoring. To perform this monitoring, ACER could organise to consult with other public authorities, and there would therefore be no need as such for the Monitoring Body in the framework of this NC.

11 Do you think the Benchmarking approach, as described in Article 13, is an adequate tool to assess whether current investments in cybersecurity to protect cross-border electricity flows are sufficient?

Not Answered

If your answer is "No", please elaborate:

12 Do the overall timelines within the Network Code on Cybersecurity seem reasonable?

No opinion

If your answer is "No", please elaborate:

The timeline of two-year cycles seem in principle reasonable to deal with a fast changing landscape of cybersecurity. However all the actions that need to be undertaken in that period of time under the risk assessment, are many and complex. This could especially affect new market entrants. See answer below.

Title II: GOVERNANCE FOR CYBERSECURITY RISK MANAGEMENT

13 Is it reasonable that the entities involved can perform the following tasks within the time set in the network code, given resource, capability, or other constraints?Activities led by the CS-NCA and NRA:a) CS-NCA and NRA to perform the member state risk assessment within 3 months (Article X)b) CS-NCA and NRA to make a transitional list of high-impact and critical-impact entities within 6 months after receiving the transitional ECII (Article Y)c) CS-NCA and NRA to identify high-impact and critical-impact entities within 6 months after receiving the ECII (Article Z)Activities performed by entities:d) High-impact and critical-impact entities to report the results of their risk assessment in 6 monthse) High-impact and critical-impact entities to implement the minimum and advanced cybersecurity controls in 6 months after their publicationf) High-impact and critical-impact entities to provide evidence of verification of the controls in 24 months after their publication

No per activity

Do you have any additional comments on the timelines:

With regard to the activities led by the electricity entities, there are many tasks involving a great number of stakeholders. We are concerned that all these tasks could be challenging to fit within a 2 years cycle.. Given that two years seems like a reasonable timeframe to keep up with the fast-changing technology developments we suggest a simplification of the corresponding workflows.
In practice, with the current proposal for activities performed by entities:
d) for the risk assessment: the timeline is too short, and probably difficult to comply with;
e) for the compliance with the minimum and advanced cybersecurity controls: we could not say whether the timeline is appropriate as we do not know at this stage what those controls would be;
f) for the provision of evidence of the controls: it would here also be too early to say whether 24 months woul be sufficient for verifying the compliance with controls which we do not know at this stage.

14 Is the proposed governance for cybersecurity risk assessment clearly described and sufficient to meet the objectives of the network code on cybersecurity?

Not Answered

If your answer is "No", please let us know what could be improved?:

Title III: RISK MANAGEMENT AT UNION AND REGIONAL LEVEL

15 Under the network code draft, cybersecurity risk assessments are performed at four levels: Union-wide, regional, member state, and entity. By integrating information from these four levels, it should be possible to get a comprehensive view on the risks. How effective do you think this multi-level process will be in assessing and reducing the cross-border cybersecurity risks in the European electricity sector?

Effective

If you think the process is not effective, how can it be improved?:

The proposed system seems to be effective. The risk assessment at four levels would lead to a clear view of the state of cybersecurity at the different levels.
However, this risk assessment at four levels might be too complex and resource intensive.
As a first step to streamline the process while maintaining its 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 there could be clear synergies and gains in efficiency. Overall we suggest to define harmonised tools and metrics to correcly manage the four different levels of risk assessment without causing added burdens to entitites that already have a compliant methodology.

How do you think the efficiency of the risk assessment process could be improved?:

16 The proposed scope of the cybersecurity risk assessments is the risks of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. Legal, financial or reputational damage of cyber-attacks are out of scope. Do you think this is a good scope to manage the cybersecurity risks to cross-border electricity flows?

Not Answered

If not, what should be added to or removed from the scope?:

17 Under the proposed cybersecurity risk management process, ENTSO-E and EU DSO with the RCCs make and approve a risk treatment plan. In approving the plan, they could be seen to accept the residual risks. Do you think this is an appropriate process for accepting the residual risks?

Not Answered

If not, which party should be responsible for accepting the residual risk at regional level?:

18 Is the proposed risk management at union and regional level clearly described and sufficient to meet the objectives of the network code on cybersecurity?

Not Answered

If your answer is "No", what could be improved?:

Title IV: COMMON ELECTRICITY CYBERSECURITY FRAMEWORK

19 Are the minimum cybersecurity controls for supply chain security in Article 24 (2) clear and sufficient?

No

If not, how should they be amended?:

The wording of Art 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 regards to the procurement requirements for the supply chain as referred to in Art 35(2), we understand that ENTSO-E and the EU DSO entity would develop harmonised cybersecurity procurement requirements in accordance with Art 35 and that those would not be made mandatory. Electricity entities would still be allowed to develop their own cybersecurity procurement requirements. However, it is uncluear what is the margin of manœuvre left for electricity entities to define their own cybersecurity procurement requirements and still be compliant with the minimum requirements listed in Art 24(2)(a)(i) to (ix). For this reason smartEn suggest ENTSO-E and the EU DSO entitiy to clearly state which requirements should be mandatory and develop a catalogue of requirements, in cooperation with market parties, from which entities could chose from depending on their risk level. Industry in particular must participate on the definition of the requirements for correctness and feasability. Special attention should be paid on the supply chain processess to avoid fracture between EU market participants requirements to suppliers.

20 The supply chain controls now require entities procuring new products and systems to set and enforce security requirements to suppliers. Should the network code also include controls that directly require suppliers to take certain measures?

Not Answered

If your answer is "Yes", please write what measures should be required from suppliers:

21 The network code proposes cybersecurity hygiene requirements in Annex A to ensure that all entities that can affect the cybersecurity of the electricity grid have a baseline security. Do you think the proposed hygiene requirements are appropriate for reducing cross-border cybersecurity risks?

Not Answered

If your answer is "Yes", please write how should the requirements be rephrased:

22 Is the proposed common electricity cybersecurity framework clearly described and sufficient to meet the objectives of the network code on cybersecurity?

No

If your answer is "No", please write what could be improved:

In its current shape, the common cybersecurity framework is neither clear nor sufficient to achieve the objectives of the NC.

The "Common CS Framework" will be composed of minimum and advanced controls. There is however no detail for the moment in the draft NC CS on the list of what constitute minimum and advanced controls. Those controls are meant to be defined at a later stage by ENTSO-E. Since minimum and advanced controls could have a significant impact on the obligations of the electricity undertaking, we believe that it is important to have a single, clear and efficient regulatory process.

smartEn suggests to already include sufficient information in the NC CS as to the key elements composing those minimum and advanced cybersecurity controls. This would ensure accountability for ENTSO-E and the EU DSO Entity when developing new cybersecurity controls, and that actors may already have an idea of the type of controls that they will have to implement. At the very least the objective that those minimum and advanced controls aim at reaching should be explicitly stated in the body of the NC CS to provide sufficient indications to the electricity entities.
For those entities that will remain outside of the scope of High / Critical Entities, the only mandatory requirements are those indicated by Enisa. We would suggest the definition of a more fitted and ambitious requirements to comply with, ensuring alignment between NIS 2.0 and Network Code on the minimum level of cybersecurity hygiene requirements.

In addition, sufficient stakeholder participation should be envisioned and clearly defined for any minimum and advanced controls defined after the finalization of the network code, and a clear plan laid out in the network code itself, including market participants in the preocess.

Title V: RISK MANAGEMENT AT MEMBER STATE LEVEL

23 CS-NCA and NRA can appoint entities as high-impact or critical-impact even where they do not individually meet the ECII level. This allows them to appoint entities for which the aggregate impact of a group of similar entities is above the high-impact or critical-impact thresholds. Do you agree with this mechanism for dealing with groups of similar entities?

Not Answered

If not, what mechanism should be used to deal with groups of entities?:

smartEn agrees in including not-yet-defined risks in the NC, but the current wording of Art 27 is very broadly formulated. It seems to allow the CS NCA to identify additional entities as high impact or critical impact 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, with transparent criteria for classifying entities into the different categories.

We understand from the FG that the NC should be reorganised so as to ensure that there should be:
i) 3 categories of electricity entities: critical impact entities, high impact entitites and SMEs. The SMEs would fall under the scope of the NC CS even though they would only be required to comply with the hygienne requirements; and
ii) a possibility for the CS NCAs to reclassify an entity at a higher level if it meets the ECII threshold (with transparent justification criteria)

24 Is the proposed risk management at member state level clearly described and sufficient to meet the objectives of the network code on cybersecurity?

Not Answered

If your answer is "No", what could be improved?":

Title VI: RISK MANAGEMENT AT ENTITY LEVEL

25 In Article 31, the network code requires entities to report information about existing controls, threats and vulnerabilities to their national regulators (CS-NCA and NRA). The regulators then report this information to ENTSO-E and the EU DSO entity for the regional risk assessment (Article 26). The information will give a good and detailed view of the cybersecurity risks to cross-border electricity flow. But the information could also be exploited by potential threat actors if they could obtain it. Do you think the benefit of collecting the information will be large enough to outweigh the risk of the information being compromised?

No

If your answer is "No", what changes would you propose?:

At the moment, the mechanism whereby the information is collected from the entity level and transmitted successively from the national to regional to EU wide level is not clear and apparent.

We would like to highlight the following considerations:
i) The bottom up approach of collecting information is welcome; but
ii) even though it would create a detailed, granular understanding of the cyber resilience of the energy system, this approach could be creating more risks than benefits.
iii) The question remains whether this level of disaggregated information, from so many potential entities can be managed by the relevant authority in a timely fashion without overlooking important threats.
iv) Entities should have one single and clearly defined point of contact for reporting.

While sharing the information is good, it might be needed to clarify further what information needs to be reported, how it could be agregated and anonymised to ensure the protection of all actors on the system in case of leak of the information. Further clarifications on the obligations of the CS NCAs, ENTSO-E and the EU DSO Entity to ensure the cybersecurity of the tools used to collect this informaiton would be welcome.

26 Entities determine the scope of the entity level risk assessment based on the outcomes of the Union-wide risk assessment, in particular the list of Union-wide high-impact and critical-impact processes. Do you think the process for determining the entity-level risk assessment scope is clear, and that the scope will cover all assets the entity needs to support cross-border electricity flows?

Not Answered

If not, how can the scoping of the entity-level risk assessment be improved?:

27 The network code allows the CS-NCA and NRA to give derogations based on three criteria:(a) in exceptional circumstances, when the entity can demonstrate that the costs of implementing the appropriate cybersecurity controls significantly exceed the benefit;(b) The entity can provide a risk treatment plan that mitigates the cybersecurity risks using alternative controls to a level that is acceptable according to the risk acceptance criteria pursuant to Article 25.3.b. The risk treatment plan shall be verified through one of the options pursuant to Article 33.(c) The results of the risk assessment of the entity do not show any direct or indirect impact on cross-border electricity flows. Do you agree with the criteria and process for providing derogations?

No

If not, how can the derogation process be improved?:

smartEn supports the inclusion of derogation criteria, however, we think that the process should be further detailed.
With regard to the process followed for granting derogations, several modifications are required to streamline and increase the robustness and efficiency of the process:
a) A clear cost benefit analysis should be implemented to assess the alternative measures taken, and to evaluate the costs in option A.
b) there should be only one entity in charge of granting the derogation: the responsibility is currently vested in two public authority which raises questions of efficiency and of conflict resolution in case those authorities reach diverging decisions to grant or not derogations;
c) 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.
d) to ensure a level playing-field, any derogation applied to an entity should automatically apply to other entities that use the same system.

28 Is the proposed risk management at entitiy level clearly described and sufficient to meet the objectives of the network code on cybersecurity?

No

If your answer is "No", what could be improved?:

We would like to raise several comments with regards to the overall clarity of the draft NC CS:
- in Art 32 (Cybersecurity management system), the description at high level of the cybersecurity management system is good and 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 in Article 32:
i) who are "the parties affected by the security risks"?;
ii) what are the resources which are referred to in point c)?
iii) what are the "roles" which are referred ot in point (e)?

- in Art 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 entitites to ensure their compliance and conformity with their obligations.

- in Art 30.1, 6 months after entry into force may be too little time for entities to apply the minimum cybersecurity controls, 24 months are more realistic.

- in Art 34.6, it should specify that random checks may only occur 24 months after entry into force of the network code.

Title VII: HARMONISING PRODUCT AND SYSTEM REQUIREMENTS AND VERIFICATION

29 Is the proposed approach for harmonizing the cybersecurity procurement requirements and verification schemes clearly described and sufficient to meet the objectives of the network code on cybersecurity?

No

If your answer is "No", what could be improved?:

The goal of both Art 35 and 36 NC CS seems to explain that ENTSO-E and the EU DSO Entity have the right and possibility (though no obligation) to develop:
a) non-binding CS procurement requirements;
b) guidances on the union certification schemes.

Since none of the articles are meant to create actual obligations, it is not clear why those articles are in the draft NC CS in the first place.

For Art 35: It should explain in article 24 that the ENTSO-E, in cooperation with the EU DSO entity, shall have the right to develop a non binding harmonised CS procurement set of requirements respecting the parameters of Art 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 Art 8 and take into account the comments.

For Art 36: Art 24 should explain, 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 and take into account their comments.

Article 23 requires further clarification. It leaves it open for electricity entities to either use the harmonized cybersecruity procurement requirements or to define their own cybersecurity procurement requirements. Nevertheless, as there is a list of minimum procurement requirements and "non binding" cybersecurity procurement requirements, it is not clear what the margin of manoeuvre for the electricity entities would be.

Title VIII: ESSENTIAL INFORMATION FLOWS INCIDENT AND CRISIS MANAGEMENT

30 Article 37 request CS-NCA to provide electrity entities with information on cybersecurity indicents, threats, and vulnerabilities to enhance the electricity entities' defense.Do you agree that the network code will help electricity entities to receive effective and adequate information to increase their threat awareness and ability to handle cybersecurity incidents?

Not Answered

If your answer is "No", what should be changed in the information sharing process?:

31 Article 39 and Article 40 present the support electricity entities receive in the event of an incident (Art.39) and crisis (Art.40).Do you think that enough support is provided?

No

If your answer is "No", how should the support be reinforced?:

Art 39 and Art 40 are 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. We support the intention to provide support, but it is not clear how this support could materialise and it is therefore doubtful that any help would actually be provided. We ask for a clear definition of the processes to request support and in which form and timeframe this will be provided.

32 Is the proposed approach for essential information flows and crisis management clearly described and sufficient to meet the objectives of the network code on cybersecurity?

Not Answered

If your answer is "No", what could be improved?:

Title IX: ELECTRICITY CYBERSECURITY EXERCISE FRAMEWORK

33 Article 41 requires critical entities to perform two exercises every three years.Do you have the capabilities to perform the mandatory cybersecurity exercises?

Not Answered

If your answer is "No", how frequently should exercises be held?:

34 Is the proposed electricity cybersecurity exercise framework clearly described and sufficient to meet the objectives of the network code on cybersecurity?

Not Answered

If your answer is "No", what could be improved?:

Title X: PROTECTION OF INFORMATION EXCHANGED IN THE CONTEXT OF THIS DATA PROCESSING

35 Are the principles and implementation rules for protection of information adequate to protect classified and sensitive information to be exchanged in a trusted way?

No

If your answer is “No”, which principles and/or implementation rules should be removed, added or modified?:

smartEn believes that significant work is still needed to ensure a robust protection of information:
- Art 46 lists principles in view of protecting the information which needs to be exchanged in the framework of the NC, but without clear indication of what the principles mean in practice nor on who lies the obligation to respect those principles. Art. 46 could establish clearer obligations with clearly identified adressees. Art. 46 should also consider a clear roadmap to be followed by the actors when handling information. For instance, it should not be for the addressees of the NC CS to wonder how to ensure their compliance with the already existing other pieces of legilsation on data protection (protection of commercially sensitive data, confidential information and trade secrets, Regulation (EU) 2016/679 and Regulation (EU) 1227/2011) but the NC CS should provide a framework which ensures that there is no conflict with those other pieces of legislation.

- Art 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.

The list of critical risk entities, the list of identified critical perimeters and systems, the cross-border electricity cybersecurity risk assessment report, and the common electricity cybersecurity framework shall explicitly be protected as European Union Classified Information (EUCI) or the applicable equivalent national classification. This information shall be protected according to Title X (Article 46(5)(a)) and 47(4) and not be made available publicly (e.g. on websites), to reduce the risk of malicious actors getting access to this information.

36 Is the proposed protction of information exchanged in the context of this data processing clearly described and sufficient to meet the objectives of the network code on cybersecurity?

Not Answered

If your answer is "No", what could be improved?:

General

37 Do you see any areas where the network code on cybersecurity can be aligned better with the revised NIS directive now under development?

Please elaborate:

smartEn would like to highlight the importance of having the CS NC and the NIS 2 directive fully aligned to avoid creating two different frameworks that are not coherent or consistent with each other. For this reason we ask for more time to be given to ENTSO-E and/or ACER to monitor and ensure the coherency of both the NIS 2 and the proposed NC CS. Apart from the alignment of timings for their adoption which could prove beneficial for the implementation of the obligations of the NC CS and to ensure that the necessary cross-references can be inserted in the NC CS, we believe it is key to ensure that those texts do not create duplicate or contradictory obligations for the different actors of the electricity sector, among others with regard to the reporting obligations
Furthermore, some areas that need to be aligned are the scope of both legislastions, in particular as to which entities it affects, and the definition of the entities and full alignment on the applicable obligations.
Regarding the scope of the CS NC and following what is already included in NIS 2 directive, the network code should be expanded to include more entities, that could pose a risk even if not directly participating in the energy system, for example E-mobility service providers (EMSP), heatpump and inverter manufacturers.
Beyond the expanded monitoring from ACER, we think that the CS NC should not be finalised before the cybersecurity framework is set under NIS 2. the CS NC should ensure harmonisation with NIS 2.0 Directive to avoid duplicated and heterogeneous obligations. For example:
- create a unique incident notification procedure
- enforce alignment of cybersecurity obligations (requirements and controls) that are adopted at national level
- promote the NC as the basis in cybersecurity for EU electricity sector, not limited to cross-border aspects.

38 Do you have any other comment you want to share and that are not included in the previous questions, with regard to the draft network code on cybersecurity?

Please elaborate:

smartEn acknowledges the paramount importance of a high level of cybersecurity for the energy sector in general, and for demand-side flexibility in particular. In order to be successful, innovative solutions need trust from society and politics. smartEn has repeatedly asked for a thorough involvement from stakeholders in the development of this legislation, and for this reason we appreciate the opportunity to participate in this consultation and in the development of the CS NC.

However, smartEn has concerns on the overall scope and development process of the CS NC. While we appreciate the complexity of such a piece of legislation, and the time-constraints that come with it, we think that the current approach of drafting a high-level network code that includes numerous delegations for different articles and details could lead to an extended implementation timeline in which stakeholders are not involved.
smartEn supports the creation of a network code that is as detailed as possible, and that delegates where necessary to different expert groups at a later stage. However, the conditions and contents should be clearly defined in the NC as well as ensuring the participation of all stakeholders in that drafting process, in the same way that they participate in the drafting process of the NC. Stakeholder participation is integral to a network code of this nature, in particular because the core content, cybersecurity, has a significant impact on market participants, and they are better suited to provide insight into the risks they might be exposed. The current draft already considers a working group to support ENTSO-E and EU DSO Entity in the elaboration of those detailed deliverables. This consideration should also include a detailed description of the composition and governing rules of these working groups. If this can't be guaranteed beforehand, we suggest to remove the possibility of this working group and proceed, similar to other NC, with clear articles on consultation procedures, stakeholder involvement, and on regulatory approvals.

Finally, the CS NC should rely on existing, tested and complementary families of standards in order to cater in an appropriate way for all the different actors of the electricity system. The interoperability of cybersecurity requirements and standards should also be addressed in the network code to avoid any vendor lock-in risk through the cybersecurity standards.

The following standard families should be used for different purposes without mandating their adoption as the unique certifiable standard. This standard list could be used for constituting the Electricity Requirements and Standards Mapping Matrix (ERSMM), following active participation from all entities in this mapping exercise, as foreseen in the ACER framework guidelines on the cybersecurity network code to preserve investment and security plans already in place in Member States:

• ISO27000 family for ICT management,
• IEC 62443 family for ICT products.