Evaluation of comments received on the Network Code on Cybersecurity during the Public Consultation

Draft | 3 February 2022

TABLE OF CONTENTS

[Introduction 3](#_Toc91844322)

[Overall summary of comments received 4](#_Toc91844323)

[Overview of Network Code Cybersecurity commentes 4](#_Toc91844324)

[Next steps 30](#_Toc91844325)

Introduction

In accordance with Article 59(9) of Regulation (EU) 2019/943 of 5 June 2019 on the internal market for electricity[[1]](#footnote-2), the European Commission requested ENTSO-E to submit a proposal for a Network Code on Cybersecurity aspects of cross-border electricity flows, including rules on risk assessments, common minimum requirements, planning, monitoring, reporting and crisis management, and a clear definition of the roles and responsibilities of the different actors for each activity.

In its letter dated 23 July 2021, the European Commission requested ENTSO-E, in a strong collaboration with EU DSO entity, to submit the proposal for this Network Code on Cybersecurity (NCCS) by 14 January 2022.

Following quality, inclusivity, and transparency requirements, on 12November, ENTSO-E together with EU DSO entity opened a public consultation on the draft Network Code on Cybersecurity (“Public Consultation”) until 10 December 2021. During this consultation period, stakeholders, and general public (“Stakeholders”) were invited to read, review and provide comments on the Network Code draft. ENTSO-E, in collaboration with EU DSO entity, organised two Stakeholder Workshops on 19November and 08 December 2021 which gathered a large amount of attendees and proved to be a great success for Stakeholder involvement and interest in the topic.

In this report, ENTSO-E, with a collaboration with EU DSO entity, summarises comments received during the Public Consultation period and provides an in-depth response to the issues raised.

Overall summary of comments received

The draft Network Code on Cybersecurity was open to Public Consultation from 12November to 10December 2022 on the ENTSO-E public consultation hub <https://consultations.entsoe.eu/system-operations/network-code-on-cybersecurity/> .

50 Stakeholders submitted their comments to the Public Consultation out of which 24 Stakeholders chose for their inputs to be kept confidential.

The comments were analysed and addressed by ENTSO-E and the EU DSO entity cybersecurity experts and taken into account in the final proposal that was submitted to the European Union Agency for the Cooperation of Energy Regulators (ACER) on 14 January 2022.

Overview of COMMENTS on the Network Code ON Cybersecurity

Question: “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?

- Please select one answer only”

Out of 50 submissions, 11 Stakeholders responded that the sector-specific rules are clear enough. 34 Stakeholders selected “no” as an answer, indicating that the rules are not clearly enough described. One Stakeholder marked “no opinion” and 4 Stakeholders did not answer the question.

Summary of the comments:

* many Stakeholders stressed the importance of aligning the proposed Network Code on Cybersecurity with the NIS 2 Directive to avoid overlapping;
* multiple Stakeholders voiced, that some definitions, such as “cross-border flows” and “cyber incident” are lacking in-depth explanations and detailed digest;
* some Stakeholders expressed an opinion that, in some parts, it is not clear by whom the objectives of the proposed NCCS shall be fulfilled;
* several Stakeholders emphasised that some energy producers and external providers fall out of the scope of the proposed NCCS which might cause vulnerabilities and risk to other market participants;
* one Stakeholder raised a question on how compliance and cooperation with neighbouring third countries will be set, this will set an important outline for the next steps on securitisation and collaboration within electricity sector;
* some Stakeholders indicated that the basic cybersecurity hygiene requirements are not of sufficient level whilst some Stakeholders emphasised that the basic cybersecurity hygiene requirements should not be a part of the proposed NCCS;
* some Stakeholders indicated that the scope and impacts on micro and small DSOs require further clarification;
* one Stakeholder emphasised the need to support mechanisms for the development of compatible cybersecurity framework and incident response capacity related to cross-border electricity flows in the physically interconnected neighbouring countries, and prospects for their integration in the corresponding cybersecurity environment in the EU.

**Development (Drafting) Team response:**

The objectives listed in the Network Code are highly inspired by the ACER framework guideline and the need to mention the correlation of the provisions on the Network Code and existing legislation on cybersecurity, risk preparedness and electricity matters. The description of the objectives was improved based on the comments received.

The Network Code also aligns as much as possible with the NIS Directive (2016). However, as the revision of the NIS Directive (NIS2) is still ongoing and there was no agreement yet between the European co-legislators, the NIS2 proposals could not be referred to in the current proposal that was submitted by ENTSO-E and the EU DSO entity to ACER. Nevertheless, as the development process of the Network Code will enter into its next phase, alignment with NIS2 Directive should be ensured progressively before the Network Code enters into force.

Definitions were constantly revised and checked for consistency as many of the definitions used in the Network Code are already defined in existing legislation e.g. ‘cross-border electricity flow’ is defined in Regulation (EU) 2019/943. A definition of ‘incident’ was added in the Network Code text but will most probably have to be aligned once the NIS2 proposal is close to final.

The scope of the Network Code was revised being more specific on the cybersecurity and cross-border aspects of the proposed sector specific provisions.

Regarding third country cooperation, the cooperation was limited to the TSO level taking into account the comments from stakeholders that DSOs will rather unlikely have relations with third country DSOs that will have an impact on cybersecurity aspects of cross-border electricity flows. The provisions on EU TSO cooperation with third country TSOs are taken from similar already existing provisions in Regulation (EU) 2017/1485.

Question: “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 Annex A within 12 months after entry into force of this Regulation." Based on the statement above, are twelve months a reasonable timeframe?

- Please select one answer only”

Out of 50 submissions, 9 Stakeholders responded positively that this is a sufficient timeframe for implementation of the basic cybersecurity hygiene requirements. 25 Stakeholders responded negatively to the question. 9 Stakeholders had no opinion and 7 did not answer.

Summary of the comments:

* one Stakeholder suggested a timeframe of 18 months. Several Stakeholders suggested that 12 months are not sufficient and a timeframe of 18 to 24 months would be more feasible;
* multiple Stakeholders emphasised that, without defining threshold for the micro or small sized enterprises, it is impossible to comment on the adequacy of the suggested implementation timeframe;
* several Stakeholders mentioned, that in the current shape and form of the NCCS, it is not clear exactly which entities would fall under the scope of the Network Code and, therefore, it is difficult to assess whether the proposed timeframe is adequate, as well as that the implementation of the proposed timeframe might depend on availability of skilled human resources within the companies;
* some Stakeholders suggested to exclude the cybersecurity hygiene requirements as they are not part of critical cross-border processes and only concerns SMEs. SMEs are not in the scope of the NCCS. Nevertheless, other Stakeholders suggested to further strengthen the hygiene requirements.

**Development (Drafting) Team response:**

The scope of the Network Code was revised being more specific on the cybersecurity and cross-border aspects of the proposed sector specific provisions. References to definitions of a ‘small enterprise’ and ‘micro enterprise’ as defined in Directive (EU) 2019/944 were added to the Network Code. The thresholds deciding which entities are considered as high-impact or critical-impact entities will still have to be developed after entry into force of the Network Code as the deadline given to ENTSO-E and EU DSO entity to develop the Network Code itself did not provide for sufficient time to address this topic in more detail.

The implementation of the Network Code will be progressively and require necessary resources in all entities that are within the scope of the Network Code.

Based on the feedback received from Stakeholders though the consultation process, it was agreed by ENTSO-E and EU DSO entity cybersecurity experts, to exclude the cybersecurity hygiene requirements from the proposed NCCS.

Question: “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 Annex 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? - Please select one answer only

- Please select one answer only”

Out of 50 submissions, 11 Stakeholders indicated that the basic cybersecurity hygiene requirements are at the appropriate level. 7 Stakeholders indicated that the requirements are too strict. 17 Stakeholders answered that the requirements are too flexible. 10 Stakeholders had no opinion and 5 did not answer.

 Summary of the comments:

* multiple Stakeholders stated that the Network Code should clearly define what is understood by micro/small sized enterprises and which organisations would fall under the scope;
* multiple Stakeholders discussed the applicability of electric vehicles charging stations operators in regards of the scope of the proposed Network Code;
* several Stakeholders stated that the entities should not be defined by size, but by how interconnected to the system they are and by the impact caused in case of the potential attack;
* multiple Stakeholders stated that the basic cybersecurity hygiene requirements should be further strengthened and detailed. Several Stakeholders recalled work of ENISA and its "Review of Cyber Hygiene practices" work;
* multiple Stakeholders suggested that the Annex A should additionally specify:
 1) the required level for category and 2) the controls to be implemented to verify that the level of maturity is reached;
* several Stakeholders suggested that the basic cybersecurity hygiene requirements list should be further detailed. And include several additional aspects, such as:
	+ requirement to enforce protection against malicious code;
	+ install security updates as soon as possible;
	+ use strong authentication such as two-factor authentication;
	+ restrict and protect the use of system administrative permissions;
	+ disable unused services and protocols;
	+ create backups and test if the information;
	+ allow only approved equipment on the network;
	+ ensure that only approved software can be run;
	+ segment the networks and filter traffic between segments;
	+ upgrade hardware and software;
	+ ensure an ability to detect security events and cyberattacks.
* several Stakeholders suggested that further clarification on which cybersecurity requirements will be imposed on mini- and micro-entities is needed. Small sized companies have minimum or no ISMS competences and must undertake large projects with external consultants to clear up their OT service management and information security management;
* one Stakeholder suggested that the basic cybersecurity requirements are too vague. More detailed and refined requirements could be developed based on the detailed work of the ENISA in its "Review of Cyber Hygiene practices";
* in addition to the criteria for identification of the SMEs, similar criteria should be defined for assessment as critical - impact or high-impact (with relevance onto EU MSs) of the entities (not only SMSs) in EU neighbouring and interconnected systems;
* further guidance materials on how to implement these requirements should be provided.

**Development (Drafting) Team response:**

ENTSO-E and the EU DSO entity are convinced that a basic level of cybersecurity should be implemented by all entities. Nevertheless, given the limited time to develop the Network Code ENTSO-E and the EU DSO entity could not enrich the basic cyber hygiene requirements beyond to what was already published by ENISA in 2017. Therefore, ENTSO-E and the EU DSO entity decided to follow the general feedback from stakeholders to remove the proposed cyber hygiene requirements from the Network Code in order not to pre-empt the discussion between the competent institutions and the concerned stakeholders to set up such general basic requirements when revising the NIS Directive.

For clarification, the definition of a ‘small enterprise’ and ‘micro enterprise’ are already defined in existing legislation (as defined in Directive (EU) 2019/944). Thus, the Network Code does not propose an alternative one. With regard to other entities (e.g. electric vehicle charging station etc.) it depends on their ECII and on the risk assessment whether they are in the scope of the Network Code and if yes, what provisions they shall apply.

Question: “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?

- Please select one answer only”

Out of 50 submissions, 8 Stakeholders indicated that the monitoring approach defined in the draft of the Network Code Cybersecurity is effective enough. 27 Stakeholders answered that they do not consider the defined approach effective enough. 10 Stakeholders had no opinion and 5 did not answer.

Summary of the comments:

* multiple Stakeholders stated that ACER is not responsible for each entity listed in Article 2 (1);
* multiple Stakeholders noted that allocation of responsibilities between ACER and the “Monitoring Body” is not clear;
* several Stakeholders noted that ACER and the NRAs may not have sufficient expertise in this field. One Stakeholder suggested for ACER and the NRAs to interface with CERTs and CS-NCAs to capitalise on reviews and monitoring which is being already performed;
* one Stakeholder suggested that for the Energy Community countries, the monitoring role should fall on the Energy Community Regulatory Board (ECRB);
* one Stakeholder added that the reporting cycle should be aligned with the already existing audit and monitoring obligations indicated in other directives, regulations to lessen the administrative burden;
* several Stakeholders mentioned that the administrative burden for monitoring activities may be hard to sustain by small companies;
* one Stakeholder suggested, additional to the regular monitoring cycles, there should be obligatory monitoring implemented after occurrence of the big incident without a need to wait for the next monitoring period;
* one Stakeholder mentioned that in addition to malicious attacks, errors in programming also pose a threat. Therefore, in depth testing of the IT architecture should be performed.

**Development (Drafting) Team response:**

ENTSO-E and the EU DSO entity recognise that the availability of cybersecurity competences in the different bodies involved in the Network Code differ across the Union and that sharing of responsibilities with regard to cybersecurity is decided by the Member States in line with the NIS Directive.

Regulation (EU) 2021/943 entrusts ACER with the monitoring of the implementation of Network Codes and Guidelines. Therefore, ACER is the competent body to carry out the monitoring. The monitoring by ACER focus on the regular monitoring of the implementation of the Network Code itself, and not on the measures taken after specific events occurred (e.g., incidents) or resulting from the cybersecurity exercises.

Taking into account stakeholder comments, the advisory role of the Monitoring Body was clarified and a specific provision on cooperation between national authorities in a Member State was added.

Question: “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?

- Please select one answer only”

Out of 50 submissions, 5 Stakeholders indicated that the benchmarking approach is an adequate tool. 30 Stakeholders responded negatively, 9 Stakeholders had no opinion and 6 did not answer.

Summary of the comments:

* one Stakeholder noted, that without having a clear understanding if the suppliers are in the scope of this Network Code, it is difficult to assess whether current benchmarking approach is sufficient;
* several Stakeholders noted, that it is not clear how benchmarking exercises would improve the cybersecurity level withing EU;
* multiple Stakeholders stated that the average benchmarking of the costs is not a reliable indicator as it does not indicate the efficiency of the improvements implemented;
* several Stakeholders noted that the IT implementation costs are not uniform across the EU countries and, therefore, the result of the benchmarking analysis would not be effective. Differences between the Member States need to be carefully considered to allow for a meaningful comparison of data and of analytical results;
* one Stakeholder noted that it is very difficult to distinguish and separate investments in cybersecurity from other investments within companies;
* one Stakeholder noted that it is not clear how the benchmarking approach will be deployed, and which expenditure will be considered;
* several Stakeholders expressed a concern that a vast amount of potentially sensitive data is gathered but it is not explained why this data is gathered and what is done with it afterwards;
* one Stakeholder suggested that adding provisions to the NCCS which describe how gathered data and results of the analysis will be shared to the Member States and to the energy sector is important;
* one Stakeholder noted that Article 13(4) regulates possible granting of classified information without a security clearance. This can constitute as a breach of national rules for handling confidential information.

**Development (Drafting) Team response:**

ENTSO-E and the EU DSO entity share the concerns raised with regards to representativity and comparability of the costs for cybersecurity. Indeed, ENTSO-E and the EU DSO entity recognize that the expenditure for cybersecurity measures does not seem to be the correct criterion to assess the maturity of cybersecurity. Nevertheless, the ACER framework guideline explicitly mentions that such a benchmarking is to be included in this Network Code. To strike the right balance between the different positions, the scope of the benchmarking that NRAs shall carry out was adapted.

NRAs oversee collect all the data from the entities within the scope of the Network Code as mentioned in the Acer Framework guidelines. With regards to confidentiality, this Network Code already sets out that the benchmarking shall not be made public and investment data will be normalised and harmonised in order to provide benchmark of NCCS implementation efficiency.

Pursuing to article 13, information is gathered for the sheer purpose of Benchmarking and assess the cost efficiency of measures and perform comparisons between measures in terms of efficiency/adequacy.

The effectiveness of investments will be evaluated in terms of cyber risk reduction risk during entity/state/region/union level risk assessment. This means that the spending of an entity will not directly result in efficiency according to the Article 13 as efficiency of measures is still to be assessed and compared.

Question: “Do the overall timelines within the Network Code on Cybersecurity seem reasonable?

- Please select one answer only”

Out of 50 submissions, 5 Stakeholders responded positively stating that the timelines are reasonable. 36 Stakeholders indicated that the timelines are not reasonable. 6 Stakeholders had no opinion and 3 did not answer.

Summary of the comments:

* almost all Stakeholders indicated that the timelines are too ambitious and too tight;
* vast number of Stakeholders indicated that there are too many new legal requirements that are coming into force in the energy sector simultaneously.

**Development (Drafting) Team response:**

The timelines were revised flowing stakeholder comments to provide for a longer cybersecurity risk assessment cycle (3 years instead of 2 years).

Question: “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 months

e) High-impact and critical-impact entities to implement the minimum and advanced cybersecurity controls in 6 months after their publication

f) High-impact and critical-impact entities to provide evidence of verification of the controls in 24 months after their publication?

- Please select one answer only”

Out of 50 submissions, 2 Stakeholder marked “Yes” as an answer. 34 Stakeholders marked option “No per activity”, 9 Stakeholders marked no opinion and 5 did not answered.

Summary of the comments:

* multiple Stakeholders indicated that the timelines set in the NCCS are too ambitious. Many Stakeholders enquired for the timelines to be extended to additional two to three years;
* one Stakeholder stated that transition period is too short;
* one Stakeholder mentioned that the methodologies, perimeters, reports, frameworks, scales, and requirements still need to be developed and, therefore, it is hard to assess the real impact of the proposed Network Code.

**Development (Drafting) Team response:**

Based on the public consultation comments, the timelines were extended. The risk assessment cycle was extended to three (3) years, and the transition period to two (2) years. The timelines were reviewed for consistency.

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

- Please select one answer only”

Out of 50 submissions, 4 Stakeholders responded that the risk assessment is clearly described and sufficient to meet the objectives of the Network Code on Cybersecurity. 31 Stakeholders answered negatively. 8 Stakeholders reviewers had no opinion and 7 did not answer.

Summary of the comments:

* multiple Stakeholders indicated that the described cybersecurity risk assessment is not clear nor sufficient;
* multiple Stakeholders stated that the risk assessment methodologies are of sufficient level, nevertheless they are too vague and further need to be elaborated; In particular, the clarification on which entities are to fulfil which obligations and in what timeframes;
* one Stakeholder indicated that the governance is clearly described only on the entity level;
* few Stakeholders stated that they would welcome more explicit text in the NCCS on proactive involvement and consultation of inter alia the CS-NCAs in the methodologies creation process. For example, in Articles 5 and 8;
* several Stakeholders commented on the “Cybersecurity risk working group”:
	+ as the Working Group shall be entitled to adopt the methodologies, it was suggested that the governance should contain a clear decision-making process based on unanimity;
	+ one Stakeholder suggested not to create the “Cybersecurity Risk Working Group” and of the “Monitoring Body”;
	+ several Stakeholders asked how ENTSO-E and EU DSO Entity will acquire the funding for the “Cybersecurity risk working group” to ensure quality in performing the duties described in NCCS. It was also pointed that proposed NCCS does not pose any legal obligations to allocate additional funding for the participants.
* it was stated that end of the transition period should be clearly stated in the Network Code.

**Development (Drafting) Team response:**

The cybersecurity risk assessment methodologies will be developed after entry into force of this Network Code.

The CS-NCAs will be involved in the development of the risk assessment methodologies through their participation in the Monitoring Body.

The cybersecurity risk working group will only be only supporting ENTSO-E and the EU DSO entity. It will not have a decision power on its own, thereby no decision-making process is required.

Alternatives to the working group and monitoring body were considered, nevertheless ENTSO-E and the EU DSO entity believe that the setup provided in the proposed Network Code is the most efficient and effective way to support ENTSO-E, the EU DSO entity and ACER with the required cybersecurity expertise.

ENTSO-E and the EU DSO entity`s funding is provided by their members. Other participants in the working group will need to bear their own costs.

The transition period ends with the start of the first risk assessment cycle as described in Article 17.

Question: “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?

- Please select one answer only”

Out of 50 submissions, 2 Stakeholders indicated that the multi-level risk assessment process is very effective. 19 Stakeholders indicated that the process is effective. 14 Stakeholders answer that the process is not effective whilst 11 Stakeholders had no opinion and 4 did not answer.

Summary of the comments:

* several Stakeholders stated that a four-layer system seems to be too complex;
* one Stakeholder suggested that on the entity level certain information should not be shared outside of a national level;
* several Stakeholders voiced concerns over the data collection process. The data reporting process can be too burdensome. The type of data gathered should be further specified.

**Development (Drafting) Team response:**

ENTSO-E and the EU DSO entity agree that the process is complex. No simplifications could however be found that would still meet the principles in the ACER framework guideline.

Entity specific information does indeed stay at Member State level. Only aggregated information is reported by the CS-NCAs for the regional risk assessments.

The information gathered was further worked out in the revised version of this Network Code.

In addition:

* several Stakeholders pointed out a need to avoid duplication of obligations to assure efficiency. Some of the Stakeholders stated that the body of data requested to be gathered is in too broad;
* several Stakeholders stated that each level should limit the information shared to need-to-know principle and in an aggregated manner.

**Development (Drafting) Team response:**

ENTSO-E and the EU DSO entity agree that duplication of obligations should be avoided. Nevertheless. it is impossible to fully exclude the possibility of duplication. The revised NIS Directive (NIS 2 Directive) is still under development, thereby the final obligations under this Directive are not known yet. In addition, no obligations under national legislation could be fully considered as national legislation differs widely across the Member States.

ENTSO-E and the EU DSO entity ensured that information is only shared on a need-to-know basis. Meaning that only information needed for the cross-border electricity cybersecurity risk assessment report is gathered. This information is aggregated already at entity and Member State level to limit the risk that the information could potentially be compromised.

Question: “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?

- Please select one answer only”

Out of 50 submissions, 21 Stakeholders responded positively to the above-mentioned question. 16 Stakeholders responded negatively. 6 Stakeholders had no opinion and 7 did not answer.

Summary of the comments:

* several Stakeholders suggested to:
	+ further include financial and reputational damage, legal violation to the security;
	+ carry out a “Business Impact Analysis”.
* one Stakeholder commented that, in their opinion, the legal basis of this Network Code limits its applicability to cross-border electricity flows.

**Development (Drafting) Team response:**

ENTSO-E and the EU DSO entity cybersecurity experts believe that reputational and legal damage should not be in the scope of this Network Code. As such, damage would not affect cross-border electricity flows. Entities should consider such damages in their own risk assessments. The risk assessment methodology at entity level allows entities to consider additional impact categories, as long as they consider the impact categories defined in this Network Code.

The approach described for the Union-wide cybersecurity risk assessment is similar to a business impact assessment, except that it is performed at a Union level, rather than at an entity level.

Question: “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?

- Please select one answer only”

Out of 50 submissions, 14 Stakeholder responded positively to this question. 14 Stakeholders responded negatively. 13 Stakeholders had no opinion and 9 did not answer.

Summary of the comments:

* several Stakeholders noted that the residual risk acceptance should firstly be approved at a national level;
* one Stakeholder noted that they believe that the national authorities decide on what are critical entities and what groups of entities become critical;
* some Stakeholders noted that the RCCs are in the right positions per Regulation (EU) 2019/943) to estimate acceptable level of residual risk, while other Stakeholders expressed concerns, that RCCs do not have the capabilities nor the authority to accept regional cybersecurity residual risks.
* contradictory comments from various Stakeholders were submitted on the risk treatment plans and residual risks. While some Stakeholders expressed an opinion that the NRAs should accept the approach, other Stakeholders expressed a view that these should be agreed between the TSOs and the RCCs;
* one Stakeholder expressed an opinion, that there should be clear criteria on which risk levels are to be mitigated and which can be considered as acceptable. ACER should approve risk treatment plans.

**Development (Drafting) Team response:**

The risk acceptance process was adjusted so that all regulatory authorities of the concerned system operation region are obliged to approve the regional risk treatment plan.

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

- Please select one answer only”

Out of 50 Stakeholders, 8 Stakeholders responded positively to this question. 17 Stakeholders responded negatively. 17 Stakeholders had no opinion and 8 did not answer.

Summary of the comments:

* some Stakeholders encouraged the current state of work and expressed their satisfaction on the proposed risk management process, whilst other did not fully agree with this statement;
* one Stakeholder noted that it is difficult to assess the risk management described in this Network Code as the corresponding methodology has not yet been drafted.

**Development (Drafting) Team response:**

ENTSO-E and EU DSO entity cybersecurity experts invested in elaboration and development of the risk management processes as much as possible. If further elaborations on the proposal are needed, they can be re-considered in the next phases of the NCCS development.

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

- Please select one answer only”

Out of 50 Stakeholders, 9 Stakeholders responded positively to this question. 30 Stakeholders responded negatively. 5 Stakeholders had no opinion and 6 did not answer.

Summary of the comments:

* several Stakeholders suggested to ensure that the ISO/IEC standards and controls are properly used to ensure supply chain security;
* some Stakeholders pointed out that background verification checks on all the staff of the supplier is not a realistic goal;
* one Stakeholder noted that future mandatory EU verification schemes will restrict entrepreneurial freedom and may create a barrier to innovation;
* it was pointed, that wording of Article 24 is to be improved;
* another Stakeholder pointed out that it was not clear if points i) to ix) of Article 24(2)(a) should also be included in the harmonised cybersecurity procurement requirements developed under Article 35. The process for procurement requirements must be very clear and transparent.

**Development (Drafting) Team response:**

The supply chain controls have been aligned with ISO/IEC 27002. Following the ACER framework guideline, the Development (Drafting Team) of this Network Code chose not to prescribe a standard.

Background verification checks do not have to be performed on all supplier staff, only to staff with access to sensitive information or access to high-impact or critical-impact entities. The amount of such staff should be kept as limited as possible. The level of background verification checks depends on the risks.

The use of certified ICT products, ICT services and ICT processes is not mandatory. Entities may organise their own verification activities. ICT products, ICT services and ICT processes used as critical-impact assets must however be sufficiently verified.

It was clarified that the harmonised cybersecurity procurement requirements in Article 35 must include all points under Article 24 (2).

Public Consultations will be held allowing all Stakeholders to participate in the development of the harmonised cybersecurity procurement requirements as set out in Article 35 of this Network Code.

Question: “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?

- Please select one answer only”

Out of 50 Stakeholders, 27 Stakeholders responded positively to this question. 7 Stakeholders responded negatively. 10 Stakeholders had no opinion and 6 did not answer.

Summary of the comments:

* majority of the Stakeholders emphasised a need to impose obligations directly on the suppliers that provide services to entities;

It mused be ensured that the suppliers should have cybersecurity by design and thoroughly tested equipment;

* several Stakeholders pointed to the importance of measures towards non-EU suppliers and to ensure non-discrimination of the EU suppliers;
* one reviewer suggested usage of ISO27001 certification or similar;
* one Stakeholder acknowledged the importance of using mechanisms for harmonised requirements, thereby, NCCS scope should not be expanded and the detailed requirements should be added in the upcoming Cyber Security Act.

**Development (Drafting) Team response:**

Security measures for suppliers were added in the revised version of this Network Code. as supported by most Stakeholders during the Public Consultation phase and is in line with the ACER framework guideline.

The definition of critical service provides was updated. Suppliers of products were included in line with the ACER framework guideline. The relation with critical-impact processes was clarified.

Non-EU suppliers are covered by Article 2 (3). It is, however, impossible to address the full complexity of this topic in this Network Code.

The specific requirements to suppliers are based on the ENISA report “Threat Landscape for Supply Chain Attacks”, and the IEC 62443 standard. Critical service providers would be considered critical-impact entities, thereby, they would have to implement a cybersecurity management system, for instance following ISO/IEC 27001.

Question: “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?

- Please select one answer only”

Out of 50 Stakeholders, 11 Stakeholders responded positively to this question. 22 Stakeholders responded negatively. 10 Stakeholders had no opinion and 7 did not answer.

Summary of the comments:

* several Stakeholders commented that the requirements are too light , thus, should be further elaborated;
* one Stakeholder noted that the list of cybersecurity hygiene requirements should be thoroughly developed and aligned with international standards. Annex B is not in line with the requirements for high and critical impact entities. The addressed entities should be thoroughly identified, and, then adequate security requirements should be drafted;
* two Stakeholders commented that the SMEs have no impact on cross-border flows, any cybersecurity hygiene requirements should be removed from the NCCS;
* several Stakeholders suggested to maximise usage of ISO/IEC standards and controls and that that the hygiene requirements do not reflect a risk base approach like ISO/IEC 27001.
* several Stakeholders noted that the requirements should be aligned with the NIS Directive.

**Development (Drafting) Team response:**

ENTSO-E and the EU DSO entity are convinced that a basic level of cybersecurity should be implemented by all entities. Nevertheless, given the limited time to develop the Network Code ENTSO-E and the EU DSO entity could not enrich the basic cyber hygiene requirements beyond to what was already published by ENISA in 2017. Therefore, ENTSO-E and the EU DSO entity decided to follow the general feedback from stakeholders to remove the proposed cyber hygiene requirements from the Network Code in order not to preempt the discussion between the competent institutions and the concerned stakeholders to set up such general basic requirements when revising the NIS Directive.

For clarification, the definition of a ‘small enterprise’ and ‘micro enterprise’ are already defined in existing legislation (as defined in Directive (EU) 2019/944). Thus, the Network Code does not propose an alternative one. With regard to other entities (e.g. electric vehicle charging station etc.) it depends on their ECII and on the risk assessment whether they are in the scope of the Network Code and if yes, what provisions they shall apply.

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

- Please select one answer only”

Out of 50 Stakeholders, 5 Stakeholders responded positively to this question. 32 Stakeholders responded negatively. 7 Stakeholders had no opinion and 6 did not answer.

Summary the comments:

* majority of the Stakeholders pointed out that the current NCCS draft does not include minimum and advanced security controls which should be the basis for the common electricity cybersecurity framework;
* several Stakeholders underlined the importance of including:
	+ OT side on the controls;
	+ remote access to assets by the entity itself of by third parties must be addressed;
	+ framework components related to risks stemming from neighboring countries and systems;
	+ framework components to be requested from / recommended to the neighboring countries;
	+ clear distinction between high-risk and critical-risk entities and high-risk and critical-risk perimeter;
	+ clarity on how the background checks should be done and who should perform them;
	+ definition of cyber-incident.
* one Stakeholder suggested to include obligation to notify in case of incident or vulnerability for suppliers of high and critical impact entities.
* several Stakeholders stressed importance of keeping the common electricity cybersecurity framework resilient;

Stakeholders were also concerned with the amount of work that would be required to update it;

* one Stakeholder stressed the importance of having a clear indication on common certification requirements;
* it was also mentioned that further clarification on classification impact on micro and small sized DSOs is needed along with assessment on cost impact on these organisations.

**Development (Drafting) Team response:**

All remarks are well noted. The outcome of the risk analysis will also provide a good indication on relevant points and will be used for updates.

Question: “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?

- Please select one answer only”

Out of 50 Stakeholders, 17 Stakeholders responded positively to this question. 17 Stakeholders responded negatively. 9 Stakeholders had no opinion and 7 did not answer.

Summary of the comments:

* several Stakeholders noted that the ECII is not defined and grouping of smaller units is not comprehensible;
* several of the Stakeholders stressed importance of including clear legal criteria needed to define an entity as high or critical impact entity;
* several Stakeholders expressed concerns, that delegating the competence to define the scope of applicability through an implementation process is likely to result in uncertainty and accountability issues;
* several reviewers suggested:
	+ three categories of electricity entities: critical impact entities, high impact entities and small and micro enterprises. Small and micro enterprises would fall under the scope of the NCCS even though they would only be required to comply with the hygiene requirements;
	+ a possibility for the CS NCAs to reclassify an entity at a higher level if it meets the ECII threshold. In this way, a small or micro enterprise would fall into the and could be asked to comply with the obligations of a high impact or critical impact entity if it meets the criteria defined in the ECII threshold.
	+ entities should have a possibility to question their appointment and have the opportunity to re-assess their appointment by another, objective party.

**Development (Drafting) Team response:**

The abbreviation ECII was added to the definitions.

The legal criteria for identifying groups of entities as high- or critical-impact were clarified, thereby reducing the uncertainty.

In line with the ACER framework guideline, ENTSO-E and the EU DSO entity cybersecurity experts believe that the scope of applicability needs to be set during the implementation to accommodate changes in the smart grid and in the threat landscape.

As the cybersecurity hygiene requirements were removed, the relevant categories for the network code are high-impact and critical-impact entities. Whether a small or micro enterprises is within the scope of this Network Code, depends on its level of the cybersecurity impact index developed under Article 16 of this Network Code.

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

- Please select one answer only”

Out of 50 Stakeholders, 12 Stakeholders responded positively to this question. 17 Stakeholders responded negatively. 15 Stakeholders had no opinion and 6 did not answer.

Summary of the comments:

* several Stakeholders stated that it is impossible to provide an answer to this question at this stage as an implementation of the risk assessment at national level will depend on the content of the risk assessment methodology (among others) which is not known at this time;
* several Stakeholders noted that there is an important difference between “risk assessments” and “risk management” and that the latter is broader than the term “risk assessment” only;
* it was pointed out that likelihood is difficult to measure for cybersecurity risks;
* several Stakeholders noted that the Member States should focus on the systemic risk resulting from gathered attacks against several entities with low individual risk;
* one of the Stakeholders noted that the risk assessment exercise is to be performed at a national level will add a tremendous new efforts for CS NCA that might not have the necessary resources to carry out their tasks;
* one Stakeholder noted that Members States should exchange best-practices in risk management.

**Development (Drafting) Team response:**

The risk assessments at the Member State level will be elaborated further in the risk assessment methodology, developed after entry into force of this Network Code.

At a Member State level, only a risk assessment is performed. This Network Code does not include national risk treatment plan that would be part of risk management. Of course, most Member States will do risk treatment at their level in the context of the NIS Directive. But as the Network Code focusses on the cybersecurity risks in regards of cross-border electricity flows, ENTSO-E and the EU DSO entity believe that requiring national risk treatment plans introduces additional complexity.

Risk is a function of consequences and likelihood, and, hence, cannot be properly assessed without considering the likelihood. ENTSO-E and the EU DSO entity agree that the likelihood is complex to measure, nevertheless, this Network Code will gather additional information allowing a better estimate than the one that is possible at the moment.

The scope of the risk assessment process is designed to focus on systemic risks. The risk assessment methodology should be designed to properly assess such risks.

The CS-NCAs will be provided with most of the information needed for the risk assessment by the entities. This approach reduces their efforts. Still, this Network Code requires substantial additional efforts by different entities, including the CS-NCAs. Exchanging best practices is a good way to reduce implementation efforts. ENTSO-E and the EU DSO entity believe that this can be done through existing collaborations between CS-NCAs that are being set up under the NIS Directive (such as the NIS Cooperation Group Work Stream 8).

Question: “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?

- Please select one answer only”

Out of 50 submissions, 8 Stakeholders responded positively to this question. 30 Stakeholders responded negatively. 6 Stakeholders had no opinion and 6 did not answer.

Summary of the comments:

* majority of the respondents noted that the risk outweighs the potential benefits.

**Development (Drafting) Team response:**

ENTSO-E and the EU DSO entity agree with the comment. This Network Code has been edited to ensure that entities no longer need to report information on threats and vulnerabilities. Information on these topics is now gathered through the data collection in Title VIII of this Network Code, so that it can still be reported in the Cross-border electricity cybersecurity risk assessment Report.

Question: “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?

- Please select one answer only”

Out of 50 submissions, 9 Stakeholders responded positively to this question. 23 Stakeholders responded negatively. 11 Stakeholders had no opinion and 7 did not answer.

Summary of the comments:

* majority of the Stakeholders noted that from the current draft of this Network Code it is not clear what assets are under the scope, as well as the difference between critical-impact and high-impact processes;.
* several Stakeholders noted, that the thresholds and certain definitions are not clear, such as, risks, criteria and critical/high-impact business processes/entities;
* several Stakeholders emphasised that a list of critical-impact/high-impact processes/entities would be required to fully evaluate the question posed above;
* one Stakeholder argued that from the current draft of this Network Code it is not certain if the connected generators are under the scope. This should be clarified;
* one Stakeholders pointed out that implementation of the process may differ between the entities and therefore, it is very important that the templates and extensive guidelines are provided.

**Development (Drafting) Team response:**

The process for determining the entity-level risk assessment scope will be further defined by the ENTSO-E and the EU DSO entity – all comments are well noted and will be taken under consideration in further work. After further defining the transitional thresholds, standards and controls during the transitional phase, the scope and the needed processes will then be clarified by ENTSO-E and the EU DSO entity.

Question: “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?

- Please select one answer only”

Out of 50 submissions, 19 Stakeholders responded positively to this question. 15 Stakeholders responded negatively. 10 Stakeholders had no opinion and 6 did not answer.

Summary of the comments:

* multiple Stakeholders suggested that:
	+ there should be only one entity in charge of granting derogations;
	+ a deadline for granting the derogation should be inserted in Art 30, so that both the requester and the public authority can rely on an expected timeline;
	+ the process needs to be streamlined so that the electricity entities can quickly benefit from derogations and can then focus their efforts on complying with the obligations set in the NCCS.
* several Stakeholders noted that there should be a clear guidelines in which cases derogations are acceptable. These clear guidelines will prevent many (trial) derogations requests including contested decisions/lawsuits;
* one Stakeholder expressed an opinion that point (a) in the question above should not be permitted. The weakest link in the chain determines the European security level.

**Development (Drafting) Team response:**

A deadline for granting derogation three (3) months was added.

ENTSO-E and the EU DSO entity agree that the derogations process should be streamlined, and clear guidance should be provided at a later stage, after enter into force of this Network Code. First, the risk-impact matrix and cybersecurity controls will need to be worked out.

ENTSO-E and the EU DSO entity believes, that implementing costs (Article 23 point (a)) should be taken into account by the NRAs and CS-NCAs when granting a derogation as some controls may simply be too expensive to implement.

Question: “Is the proposed risk management at entity level clearly described and sufficient to meet the objectives of the network code on cybersecurity?

- Please select one answer only”

Out of 50 submissions, 9 Stakeholders responded positively to this question. 23 Stakeholders responded negatively. 13 Stakeholders had no opinion and 5 did not answer.

Summary of the comments:

* majority of the Stakeholders noted, that it is not clear if connected network customers, such as generators, are in the scope. Also, the list of processes must be clarified;
* one Stakeholder noted, that this Network Code should foresee capabilities and functionalities of the electricity undertakings necessary for information sharing;
* some Stakeholders stated, that the proposed risk management at the entity level seems to be sufficient but not clearly described;
* one Stakeholder suggested that there should be a general criteria and obligation/recommendation for establishment of a risk management mechanism for the third countries.
* several Stakeholders noted that the risk treatment plan and mitigating controls need to be presented to both the NRAs and CS-NCAs. This shares the vulnerability information with too many unnecessary parties. This paragraph should have an "and/or" (NRA and/or CS-NCA);
* one Stakeholder suggested that the Article 29.2(d) should include "residual risk acceptance";
* one Stakeholder noted that six (6) month period after entry into force of this Network Code may be too short for entities to apply the minimum cybersecurity controls. 24 months are a more realistic timeline. Additionally, the Stakeholder suggested that random checks may only occur 24 months after entry into force of this Network Code.

**Development (Drafting) Team response:**

The process for determining the entity-level risk assessment will be further defined by ENTSO-E and the EU DSO entity – all comments are well noted and will be taken under consideration in further discussions. After the transitional phase the scope and the needed processes will be much clearer.

The timeline for the risk assessment was significantly extended in the revised version of this Network Code, based on several stakeholder comments . As this Network Code on Cybersecurity is a European Regulation, its scope of application is limited to the European Union.

**Question: “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?**

- Please select one answer only”

Out of 50 submissions, 9 Stakeholders responded positively to this question. 24 Stakeholders responded negatively. 13 Stakeholders had no opinion and 4 did not answer.

Summary of the comments:

* several Stakeholders noted that the verification schemes still need to be further developed;
* one Stakeholder noted that both Article 35 and Article 36 of the NCCS seems to explain that ENTSO-E and the EU DSO Entity has the right and possibility (though no obligation) to develop non-binding cybersecurity procurement requirements and guidance on the Union certification schemes. Since none of these articles are meant to create legally binding obligations, it is not clear why these articles are in this Network Code.
* several Stakeholders asked to further clarify how these procurement requirements relate to incoming Cyber Security Act and ENISA's work.
* one Stakeholder noted that harmonised procurement requirements should be done on the EU-wide level in order to impact vendors. For example, the Baltic region is too small (3 countries, 5 million people) to do so on its own.
* one Stakeholder suggested to include relevant industry associations for the definition process.
* several Stakeholders expressed an opinion that harmonising the cybersecurity procurement requirements should only be non-binding guidelines and not enforceable rules.
* the NCCS should make it clear that the electricity entities remain free to adopt their own procurement requirements and that the procurement requirements cannot be legally binding.

**Development (Drafting) Team response:**

The guidance on certification schemes will be developed once this Network Code will enter into force. This Network Code only provides the legal framework to develop such guidance material. The NCCS is not a technical document describing the schemes themselves.

ENTSO-E and the EU DSO entity considers that it is necessary to include harmonised procurement requirements and certification guidance, even though, they do not create additional obligations to entities as they are non-binding. The revised NCCS captures the understanding that was reached among stakeholders on this topic. The Cybersecurity Act is new and the responsibilities for certification are under development. During this Network Code development process, there has been considerable discussions on the responsibilities of ENTSO-E and the EU DSO entity, concluding that this Network Code provides a solution by making them responsible for developing sector-specific guidance on the cybersecurity certification schemes ( developed by ENISA under the Cybersecurity Act).

ENTSO-E and the EU DSO entity intend to have harmonised procurement requirements throughout the European Union. This point is clarified in the revised version of this Network Code.

Industry associations will be involved through the Cybersecurity Working Group and through public consultations. More details on the planned stakeholder involvement are described in the Supporting Document of the NCCS.

Entities remain free to set their own procurement requirements and choose their own verification option. This is stated explicitly in the article on supply chain security controls.

Question: “Article 37 request CS-NCA to provide electricity entities with information on cybersecurity incidents, 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?

- Please select one answer only”

Out of 50 submissions, 17 Stakeholders responded positively to this question. 17 Stakeholders responded negatively. 12 Stakeholders had no opinion and 4 did not answer.

Summary of the comments:

* several Stakeholders responded that this Network Code will not help electricity entities to receive effective and adequate information to increase their threat awareness and ability to handle cybersecurity incidents on the European level as the implementation may vary drastically amongst Member States;
* several Stakeholders noted that responsibilities between CSIRTs and CS-NCAs should be further clarified while others emphasised that is redundant;
* several Stakeholders provided following suggestions:
	+ article 37(8) should not only foresee a feasibility study for the development of an IT tool but rather clearly plan for the development of such a tool, allocate the responsibility to such a tool to an actor, determine the key requirements in terms of availability, redundancy, resilience, back-up, functionality and cybersecurity of the tool itself and allocate sufficient funding for such a tool.
	+ in terms of applicability, it should 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 is not appropriate to ask CSIRTs to comply with these obligations if they are not realistically given the means to do so.. Similarly, it seems important to clarify what should happen in case the IT tools becomes unavailable.
* one Stakeholder noted that Article 37 should be clearer in terms of timelines;
* one Stakeholder suggested to include details on the exchange of information with the neighbouring Energy Community countries;
* one Stakeholder shared an opinion that it cannot support withholding information about zero-day vulnerabilities, as stipulated in Article 37(5). Regardless of whether the respective manufacturer has developed patches or instructions at the time the vulnerability becomes known, mitigation methods may already have been developed independently from the manufacturer. To increase information security, the competent national authorities for cybersecurity and, especially the CSIRTs, must be allowed to share this information independently from the manufacturer.
* one Stakeholder noted that wording "sharing capabilities" with other CSIRTs is vague with potential implications. It should be clarified what is meant by "capabilities";
* one Stakeholder expressed disagreement with Article 37 (d) as it is not part of the activity of CSIRT teams;
* one Stakeholder expressed an opinion that it is important to define which information has to be shared to ensure efficiency in the early warning system.

**Development (Drafting) Team response:**

Together with the NIS Directive the target of the NCCS is to achieve a certain degree of harmonisation at the European level. Nevertheless, this Network Code also provides every Member State with the possibility to take their national specificities into account. This Network Code is drafted with the main goal to improve the overall cybersecurity situation for the electricity sector in Europe. This first Network Code on Cybersecurity is the first step to harmonise on a level, with which every Member State can deal with.

ENTSO-E and the EU DSO entity explicitly added a reference to the NIS Directive in the title VIII by the new article 37, in order to, e.g., avoid double reporting. With that, all existing entities (e.g. national CSIRTs or CS-NCAs) should have the same responsibility in line with 2016 NIS Directive. Existing processes, experience and solutions for coordination or sharing of capabilities can be used. Also, other definitions are aligned with the NIS Directive, and by doing so, the topic of data protection is specifically addressed. On few topics, the NCCS provides stricter requirements than the NIS Directive in order to take the criticality of the electricity sector for the European society into account (e.g. deadlines for the exchange of information on disruptions). The entire NCCS scope is limited to cybersecurity aspects of cross-border electricity flows.

At the moment, it is not possible to describe a possible tool to support the exchange of information in more detail. In addition to more time, this requires the cooperation of the future responsible bodies (e.g. national CSIRTs, ENISA, CSIRT Network). There are already tools in use by different CSIRTs and/or by the CSIRT Network. The feasibility study is meant for assessing if any of these tools can be used in a wider area in the future or if developing a new tool is more efficient. In case the result of the feasibility study may show that such a central tool is not efficient, ENISA, who is responsible for the ECEWC, where cyber security threats against cross-border electricity flow will be disseminated to the affected entities, may decide to develop such a tool.

Regarding deadlines, ENTSO-E and the EU DSO entity proposals for deadlines on what is to be implemented, when and by whom takes into account to the overall implementation time of the NCCS.

The scope of this Network Code cannot be expanded outside the EU and dispositions applying to third parties outside of the EU cannot be added in the legal text.

Responsible Disclosure (also known as coordinated vulnerability disclosure) of a zero-day-vulnerability is a vulnerability disclosure model in which a vulnerability or an issue is disclosed only after a period of time that allows for the vulnerability or issue to be patched or mitigated on another way. This period distinguishes the model from full disclosure. After finding a mitigation measure (like a patch) a full disclosure will inform all effected entities and give them the chance to mitigate the vulnerability in their environment. A full disclosure without having a mitigation measure, gives attackers the chance to miss-use the vulnerability without the chance for effected entities to protect themselves.

Question: “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? Tom

- Please select one answer only”

Out of 50 submissions, 17 Stakeholders responded positively to this question. 16 Stakeholders responded negatively. 13 Stakeholders had no opinion and 4 did not answer.

Summary of the comments:

* stakeholders emphasised that various entities and organisations have a supporting role in the NCCS, however, it is not clear how their help can be sought for or what type of a help can be provided. This needs to be clarified.
* several Stakeholders argued that the CSNCAs or CSIRTs have to coordinate the exchange of information between CSOCs or MSSPs of different electricity entities, however, in the NCCS it is not clarified how this exchange should be organised;
* multiple Stakeholders urged to include practical examples with clear roles (RACI matrix) for incident management in the Supporting Document of the NCCS.
* stakeholders suggested that Articles 39 and 40 foresee that support can be provided to the entities. However, it is not clear how this support will be provided.
* one Stakeholder noted that the exact obligations and the exact scope of entities which will have to comply with the reporting obligation remain unclear and it should be clarified in this Network Code.
* several Stakeholders noted that most important partners in practical incident handling in addition to CSIRTs are the vendors and security service providers, thereby, It should be clarified what type of support the EU DSO entity and ENTSO E can provide.

**Development (Drafting) Team response:**

ENTSO-E and the EU DSO entity explicitly added a reference to the NIS Directive in the title VIII by the new article 37, in order to, e.g. avoid double reporting. With that, all existing entities (e.g. national CSIRTs or CS-NCAs) should have the same responsibility in line with 2016 NIS Directive. Existing processes, experience and solutions for coordination or sharing of capabilities can be used. Also, other definitions are aligned with the NIS Directive, and by doing so, the topic of data protection is specifically addressed. On few topics, the NCCS provides stricter requirements than the NIS Directive in order to take the criticality of the electricity sector for the European society into account (e.g. deadlines for the exchange of information on disruptions). The entire NCCS scope is limited to cybersecurity aspects of cross-border electricity flows.

Further information on who is responsible for what and more details on processes and functions are explained in the Supporting Document of the NCCS.. Nevertheless, some processes are still under construction and will be developed in the transitional phase together with relevant stakeholders and taking into account already existing processes (e.g. processes implemented based on the NIS Directive).

Detailed escalation and handling processes must be developed in the incident response processes of each effected entity and follow the existing processes from the CISRTS-NCA/CSIRT-Network and CyCLONe.

Supporting entities with the information on security service providers or vendors could be a task for the national authority according to specificities in each the Member State.

For the support from third parties, a contractual relationship between the entity and the security service provider or a vendor is needed. More detailed information has been included in the NCCS.

Question: “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?

- Please select one answer only”

Out of 50 submissions, 10 Stakeholders responded positively to this question. 23 Stakeholders responded negatively. 12 Stakeholders had no opinion and 5 did not answer.

Summary of the comments:

* several Stakeholders noted that specifications on which incidents are considered as “mandatory” to be reported and which ones are “recommended” to be reported should be included in the proposed NCCS;
* several Stakeholders expressed concerns that the number of information requested to share can overload involved institutions undermining implementation of this Network Code.
* one Stakeholder noted that the information flow and crisis management structure of this Network Code should include a separate level of cooperation for the Member States but also for Energy Community and neighbouring non-EU countries;
* stakeholders noted that this Network Code should be aligned with reporting requirements from other existing European legislations, in particular with the NIS Directive.
* one Stakeholders underlined that it is very important to ensure a detailed cybersecurity methodology as well as clear reporting and follow-up processes to facilitate high-quality implementation;
* several Stakeholders noted that wording of the Article 38(3) should be clarified.
* several Stakeholders noted that the information on data protection is missing;
* one Stakeholder noted that in relation to crisis management (pursuant to Article 40), this Network Code proposes changes and innovations with respect to the mechanisms already existing or being established at the EU level and in contradiction to the general structure outlined by legislation currently in force, aimed at avoiding duplication and overlapping. It is believed that these provisions should be deleted.

**Development (Drafting) Team response:**

ENTSO-E and the EU DSO entity explicitly added a reference to the NIS Directive in the title VIII by the new article 37, in order to, e.g. avoid double reporting. With that, all existing entities (e.g. national CSIRTs or CS-NCAs) should have the same responsibility in line with 2016 NIS Directive. Existing processes, experience and solutions for coordination or sharing of capabilities can be used. Also, other definitions are aligned with the NIS Directive, and by doing so, the topic of data protection is specifically addressed. On few topics, the NCCS provides stricter requirements than the NIS Directive in order to take the criticality of the electricity sector for the European society into account (e.g. deadlines for the exchange of information on disruptions). The entire NCCS scope is limited to cybersecurity aspects of cross-border electricity flows.

The scope of this Network Code cannot be expanded outside the EU and dispositions applying to third parties outside of the EU cannot be added in the legal text.

More detailed information has been included in the NCCS.

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

- Please select one answer only”

Out of 50 submissions, 10 Stakeholders responded positively to this question. 16 Stakeholders responded negatively. 18 Stakeholders had no opinion and 6 did not answer.

Summary of the comments:

* some Stakeholders expressed an opinion that these exercises should follow the top-down and bottom-up approach cycle with the following proposed timeframes: two (2) exercises every four (4) years (one exercise every two (2) years);
* several Stakeholders expressed concern over a very high workload that will result from obligations stemming from the two (2) years risk assessment cycle. Additionally, several Stakeholders expressed a concern that not all organisations have the required capabilities to perform extensive crisis exercises;
* one Stakeholder suggested one (1) exercise every three (3) years should be sufficient;
* one Stakeholder emphasised that micro or small enterprises do not have the necessary capabilities to perform such large-scale cybersecurity exercises.

**Development (Drafting) Team response:**

Two main issues were raised during the public consultation. The first one is the synchronisation of the cybersecurity exercise cycle with the risk assessment cycle. The second one is the high workload created for critical-impact entities (the only kind of entity requested to participate; small and micro enterprises are generally not expected to participate in these exercises, only if they are critical-impact entities). The two (2) years devoted to the risk assessment cycle were extended in the revised network code to three (3) years giving more time to perform the assessments and allowing the two (2) cycles (exercises cycle & risk assessment cycle) to be synchronised. At the same time, the workload concerning exercises remains the same. Nevertheless, it should be noted that it will strongly depend of the type of scenario used by the organizer (the scenario proposed by ENTSOE is not compulsory) and that the NCCS offers all the possibilities of grouping the exercises with other national or regional exercises, thus, limiting the total number of exercises. Carrying out exercises to train and prepare your entity for a major incident or crisis should be regarded as an investment in a higher cybersecurity level.

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

- Please select one answer only”

Out of 50 submissions, 13 Stakeholders responded positively to this question. 17 Stakeholders responded negatively. 14 Stakeholders had no opinion and 6 did not answer.

Summary of the comments:

* several Stakeholders stated that it is impossible to have a clear overview, at this stage, on the obligations for the electricity entities in terms of cybersecurity exercises, without the defining critical processes.
* several Stakeholders stated that a clear definition of the scope and size of these exercises should be defined, as well as responsibilities and roles.
* one Stakeholder requested detailed guidance documents to support the implementation of the exercises.
* one Stakeholder noted that a successful cybersecurity exercise is composed out of four consecutive phases post risk identification:
i) defining cyber incident scenarios;
 ii) defining the key success criteria;
iii) cybersecurity exercise and lesson learnt (via report); and
iv) compiling an action plan to include some remediation activities.
The Stakeholder expressed a concern that the current draft of the NCCS does not fully take into consideration above-mentioned steps or tend to mix them;
* one Stakeholder commented that the Article 43(2) contradicts itself and should be re-written.

**Development (Drafting) Team response:**

Even if the precise list of the critical processes is not yet official, entities already know their sensitive processes in their respective sector. The NIS Directive provided a good indication on that for each Member State. The questions to be answered by the entity is: is this sensitive process capable of having a serious impact on cross-border electricity flows if it was to be stopped fully and instantly?

The scope and size of exercises should be decided and adapted by the organizer. ENTSO-E and the EU DSO entity will propose templates and methodologies at the beginning of each cycle but organizers can adapt them to new threats or vulnerabilities. It is important to give the organizers the freedom to adapt – or even change completely - exercises to the needs of the field.

The four consecutives' phases are fully respected and described through Title IX:

* art. 44(5) & 45(6): i) definition of the scenarios and ii) definition of the key success criteria (key success criteria concept has been implemented accordingly to the comments);
* art. 44(1,2) 45(1) & 46(2): iii) running the cybersecurity exercise itself and issuing a lesson learnt report; and
* art. 46(2) & 46(3): iv) compiling an action plan to include some remediation activities.

The *Art.44(2) -* provides the possibility to NRAs to organise a national exercise in substitution to internal exercise (Art.44(1)). To be clear, critical-impact entities must conduct an internal exercise or to participate in a national one. If the NRA decides to organise a national exercise, the critical-impact entities will have to participate in it and may - if these entities want - organise an additional internal exercise.

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

- Please select one answer only”

Out of 50 submissions, 10 Stakeholders responded positively to this question. 20 Stakeholders responded negatively. 16 Stakeholders had no opinion and 4 did not answer.

Summary of the comments”:

* several Stakeholders expressed an opinion that significant work still needs to take place to ensure a robust protection of information;
* several Stakeholders suggested that sharing of sensitive data needs to be limited to absolute minimum;
* several Stakeholders noted that this Network Code must explicitly mention that the list of critical risk entities, the list of identified critical parameters and systems, the cross-border electricity cybersecurity risk assessment report, as well as the common electricity cybersecurity framework, is considered as the European Union Classified Information (EUCI) or the applicable equivalent national classification;
* several Stakeholders noted that the reporting of inventory assessments and risk assessments included in the processes is governed by national legislation that currently prevents information from being reported to the EU;
* stakeholders suggested that the Article 46 should be re-drafted to ensure that it is actionable and provides a clear roadmap to be followed by the actors when handling information;
* stakeholders noted that information handling and classification (classified vs. sensible non classified) procedures must be re-worded to add additional clarity;
* stakeholders note that the Article 47 only creates an obligation to classify information in different categories but does not explain what regime applies to those different categories of data;
* stakeholders noted that the terminology used to classify different types of confidentiality levels are should be clarified;
* one Stakeholder expressed a concern that definitions regarding the different levels of confidentiality are not clear enough.
* one Stakeholder stated that it is unclear whether Articles 47 and 48 apply to information exchanged in the context of Title VIII;
* one Stakeholder ephasised that connected MSSPs pose a risk as they might come from non-EU countries. Stricter rules on trust requirements should be applied prior to granting access to sensitive information;
* one Stakeholders suggested to completely remove information sharing requirements from this Network Code.

**Development (Drafting) Team response:**

This Network Code has been revised to state the basic principles of protection and classification while the details of classification for confidentiality, integrity and availability are to be developed during the initial risk management process and described as classification criteria and derivative protection requirements in the common electricity cybersecurity framework. This will ensure a more robust protection of information.

The mandatory information sharing pursuant to the NCCS risk management process was revised to minimise the sharing of the sensitive data, including both NCCS Classified Information and NCCS Sensitive Information. The rules for classification of information defined by the common electricity cybersecurity framework shall define in more detail which reportable information that qualifies as NCCS Classified Information and NCCS Sensitive Information. The NCCS Classified Information category defined is foreseen to include EUCI and similar Member State classification schemes, please also refer to the NCCS Supporting document. The principles of marking information are to determine and indicate the level of classification and the dissemination specification (who will be the authorised audience and what shall be the authorised purpose for disclosure). If information is classified as EUCI, the rules of Commission Decision (EU, Euratom) 2015/444 will apply. The legal text of Title X refers to this as NCCS Classified Information.

The principle that the Members States are not obliged to supply classified information is stated in recital 8 in Directive (EU) 2016/1148 (NIS Directive). In accordance with Article 346 of the Treaty on the Functioning of the European Union (TFEU), no Member State is to be obliged to supply information the disclosure of which it considers to be contrary to the essential interests of its security. The NCCS will have to respect that. The principle is referred to in the revised Article 46 of this Network Code. Please also note, that the NCCS was revised to minimise the sharing of the sensitive data. About conflict with other legislation, Title X of the NCCS is only about protection of information within the scope of the NCCS. As such, it does not evaluate the information itself but only protection rules for a defined set of classification categories. The ACER framework guideline for the NCCS requests a classification system to be defined in the NCCS. Title X of this Network Code was revised to include a more generic classification scheme for that purpose. Details are to be defined by the common electricity cybersecurity framework.

Question: “Is the proposed protection of information exchanged in the context of this data processing clearly described and sufficient to meet the objectives of the network code on cybersecurity?

- Please select one answer only”

Out of 50 submissions, 11 Stakeholders responded positively to this question. 17 Stakeholders responded negatively. 15 Stakeholders had no opinion and 7 did not answer.

Summary of the comments:

* multiple Stakeholders commented that it is unclear why ACER needs companies’ data and why this data should be collected;
* multiple Stakeholders indicated that sharing of sensitive information should be limited as much as possible;
* several Stakeholders indicated that communication should be follow TLP red classification;
* one Stakeholder commented that the scope of information flow is not clearly described in the current draft of this Network Code;
* one Stakeholder noted that this Network Code should explicitly mention that the list of high risk/ critical risk entities and the results of their risk assessments shall not be publicly available and shall be protected at minimum by a two-factor authentication measures.

**Development (Drafting) Team response:**

Why ACER needs information is defined by the ACER framework guideline for the NCCS. In the NCCS this is reflected by describing the mandatory information shared in the context of the risk management and the NCCS compliance monitoring activities. Please also note that the NCCS was revised to minimise the sharing of the sensitive data.

The NCCS was revised to state the basic principles of protection and classification while the details of classification for confidentiality, integrity and availability are to be developed during the initial risk management process and described as classification criteria and derivative protection requirements in the common electricity cybersecurity framework. The details on using TLP or similar protocols shall be defined by the common electricity cybersecurity framework, as well as rules for encryption and authentication methods.

The scope of information exchanged is defined by the scope of the NCCS, please see the recital (4) of the NCCS i.e., sector-specific rules at Union level for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management. The information flows are mainly defined by the risk management, incident handling and crisis management provisions of the NCCS.

Question: “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.”

Out of 50 submissions, 39 Stakeholders provided answer to this question:

Majority of the Stakeholders indicated that it is important to assure that the NCCS does not duplicate, overlap, or contradict but benefit and build on the NIS Directive as well as on other already existing legislation. Additionally, many Stakeholders stressed the need to avoid double reporting. It was also underlined that NCCS should be aligned with the NIS 2 Directive on the supply chain requirements.

Several Stakeholders commented that it is impossible to answer to this question at this moment as the NIS 2 Directive is still in the drafting stage. Additionally, many Stakeholders noted that further details pertaining to the implementation of this Network Code will be known after the Network Code will be adopted, through the work of the Working Groups when developing the relevant methodologies.

One Stakeholder commented that the full scope of this Network Code remains unclear and leaves too much room for interpretation. Scope of the activities (i.e. which activities performed by a given entity fall within scope) is missing and there should be explicit mention that only activities which pertain to cross-border electricity flows are in scope.

One Stakeholder proposed for the Article 2(5) to be further expanded to add a statement that entities providing services in several Member States should be supervised by a single regulatory authority of the country of establishment. For entities not established in the EU, the competent regulatory authority shall be the one of the Member State of the designated representative of the non-EU entity.

One Stakeholder commented that the costs borne by system operators subject to network tariff regulation and the costs borne by other electricity entities in scope stemming from the obligations set out in this Network Code shall be assessed by the relevant regulatory authorities. Costs deemed as reasonable, efficient, and proportionate shall be recovered through network tariffs or other appropriate mechanisms for the system operators and for the other electricity entities through the system operators.

Several Stakeholders commented on definitions of the Code and terminology mapping:

* one reviewer commented that definition of “sensitive information” is missing and should be added to the Code;
* various directives, laws, codes, etc. are using different terms.. Stakeholders suggest that in this case it would be worth to map terminology used across various documents and explain what they mean and how do they apply in the context of this Network Code.

**Development (Drafting) Team response:**

ENTSO-E and the EU DSO entity strive to algin as much as possible with existing legislation, in particular with NIS 2 Directive. Alignment with the revised NIS Directive (2.0) has to be dealt with in the later stages of the network code revision process by ACER and the European Commission as the revision of the NIS Directive was still ongoing when ENTSO-E and the EU DSO entity had to submit the Network Code proposal to ACER.

It is important to note that the NCCS only applies to cross-border electricity flows (the scope), thereby, further mentioning in each chapter would be deemed unnecessary.

The definition of “NCCS Sensitive Information” can be found in Title X. Only definitions that are NCCS specific are mentioned in the proposed Network Code, the usage of other definitions have been based on already existing legislation.

This Regulation shall apply to critical service providers not established in the Union but who deliver services to entities in the Union. Where such a critical service provider delivers services to process data, large-scale services and regular services to entities established in the Union, this critical service provider shall explicitly designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. The critical service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established. This representative may be addressed by any competent authority in the Union instead of the critical service provider with regard to obligations of that critical service provider under this Regulation.

The NCCS draft includes that the costs borne by TSOs and DSOs subject to network tariff regulation and stemming from the obligations laid down in this Regulation shall be assessed by the relevant NRAs. Costs assessed as reasonable, efficient and proportionate shall be recovered through network tariffs or other appropriate mechanisms.

Question: “Do you have any other comment you want to share and that are not included in the previous questions, with regards to the draft network code on cybersecurity? – Please, elaborate.”

Out of 50 submissions, 39 Stakeholders provided answer to this question.

Multiple Stakeholders noted that proposed timelines for risk assessment cycles are too short and should be extended.

Several Stakeholders indicated that it is crucial to assure that the NCCS does not duplicate, overlap, or contradict but benefit and build on the NIS Directive as well as on other already existing legislation.

Several Stakeholders noted the need for additional documents, such as guidelines and checklists provided to all involved parties to guide them in the implementation work of this Network Code.

Stakeholders noted that an obligation to share any information related to a reportable cybersecurity incident with CS-NCAs or CSIRTs no later than four (4) hours from the occurrence is a too short timeframe.

Reviewers suggested clarifications on the following aspects of this Network Code:

* governance;
* scope;
* framing the responsibilities and the tools to be put in place to allow exchanges of sensitive information.

Several Stakeholders noted that framework and process for risk assessment and rating of entities is unclear.

One Stakeholder suggested to either define the scope of applicability directly – by listing the electricity undertakings that fall within the scope or indirectly – through setting a methodology determining the applicability. Delegating the competence to define the scope of applicability through an implementation process is likely to result in uncertainty and accountability issues.

One Stakeholder commented that number of electric vehicles charging stations is rapidly growing. This Network Code should address and this topic to assure stability and security of the grid.

One Stakeholder noted that further work should be done to integrate the “gathered risks”. The systemic risk resulting from gathered attacks against several entities with low individual risk is real. It is important to set requirements based on functionality and processes. The top-down approach is recommended.

One Stakeholder commented that circumstances under which derogations will be granted should be further specified. Additionally, it was pointed out that no penalties for breaching this Network Code are foreseen. If penalties will be implemented, it will need to be clearly specified what institution will be responsible for deciding on them and how will they be enforced.

One Stakeholder expressed concerns over security of collected cybersecurity information and compiled reports. These are obvious targets for hackers, thereby, should be well protected and collection of minimal data is needed in order not to create further unnecessary risks.

**Development (Drafting) Team response:**

The timelines of the risk assessment cycle were extended from two (2) to three (3) years and the transitional period was adapted.

ENTSO-E and the EU DSO entity strive to algin as much as possible with existing legislation, in particular with NIS 2 Directive. Alignment with the revised NIS Directive (2.0) has to be dealt with in the later stages of this Network Code revision process by ACER and the European Commission as the revision of the NIS Directive was still ongoing when ENTSO-E and the EU DSO entity had to submit the Network Code proposal to ACER.

Concerning the timelines provided to high-impact and critical-impact entities to report incidents to their CSIRT-NCA (Art.39.3.b), the definition of the “reportable cybersecurity incident” stipulates that the 4h starts when the incident is assessed and confirmed by the authorised representative of the entity. This should provide enough time for the entity to fulfil this reporting obligation. This first report should be considered as a first notification to be followed by more information later depending on the course of the incident.

The governance of this Network Code was improved by clarifying the role of the advisory bodies, the Working Group and the Monitoring Body as well as the cooperation at Member State level between NRAs, CS-NCAs and CSIRTs.

Within the given limited time to develop this Network Code it was not possible for ENTSO-E and the EU DSO entity to define the thresholds and methodologies in the NCCS itself. Furthermore, stakeholder involvement needs to be assured when defining the thresholds and methodologies. Therefore, these deliverables will be part of the implementation phase.

Whether electric vehicle charging stations will fall under the scope of the NCCS depends on whether they are to be considered as high-impact or critical-impact entities, depending on their ECII and the risk assessment.

The criteria for derogations are included in Article 20 of the revised NCCS. It is up to the NRAs and CS-NCAs to assess whether a derogation should be granted to an entity. Regarding penalties, these are dealt with at national level as enforcement power lies with the NRAs.

Provisions regarding data protection, sharing of information and confidentiality were revised in this Network Code.

1. European Commission (2019), Regulation (EU) 2019/943 of 5 June 2019 on the internal market for electricity, Brussels, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0943> [↑](#footnote-ref-2)