DSO ENTITY
DSOs FOR EUROPE

Comments on DG ENER's version of the Network Code on Cybersecurity

15 June 2023

DSO ENTITY
DSOs FOR EUROPE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

On 24 May 2023, DG ENER shared a new version of the Network Code for Cybersecurity (NCCS). A proposal for the NCCS was first submitted by ENTSO- in cooperation with the DSO entity to ACER on 14 January 2022. ACER provided their revision on 14 July 2022. Since then, DG ENER has been reviewing the NCCS and aligning it with NIS2 Directive. The first version was shared on 22 May for commenting in the ECG. DSO Entity holds an observer position in the ECG, nevertheless, DSO Entity believes that the below mentioned aspects are of crucial importance to the TSOs and the wider electricity community. In the light of this, DSO Entity would like to ask the European Commission (henceforth the EC) to consider the comments provided.

DSO Entity fully supports the goal of the EC to align the NCCS with the NIS2 Directive. DSOs and other entities in scope already need to comply with NIS2 Directive, hence reducing the workload. DSO Entity believes that certain changes introduced by the DG ENER would inhibit the NCCS from reaching its goals. In particular:

- Extending the scope of the Union-wide and Regional risk assessments to cover also non-malicious threats would create an overlap with other risk management regulations for the electricity sector. It also creates a significant increase of resources needed to perform the analysis.
- Removing the requirement for competent authorities to share information on incidents with high- and critical-impact entities may result in the information not reaching these entities, while they are the ones that most need it. A mechanism to ensure communication and direct information exchange amongst national agencies and entities was one of the pillar of the NCCS.
- Replacing certification as an option with verification with independent audits removes some of the quality assurance mechanisms from using an official conformity assessment body. Explicit quality requirements should hence be included in the audits in order to ensure the same level of quality.
- Making the documents in the transitional period non-binding. Because of this change, national competent authorities can only identify high-impact and critical-impact entities after 57 months (almost 5 years). Before these entities are defined, none of the provisions in the NCCS are binding.

Our recommendations can hence summarize as follows:

DSO Entity's recommendations:

- Limit the scope of the Union-wide and regional risk assessments to cyber-attacks;
- Require information sharing from national agencies to entities;
- Include quality requirements on independent audits;
- Make the transitional documents binding for critical entities.

In addition, considering the evolution of cybersecurity regulations landscape since 2021 (NIS2, CRA, CSA), as well as the modifications successively integrated in the different phases of the construction of the NCCS, DSO Entity suggest the commission launching ASAP a cost / benefit analysis in order:

- To assess the added value of the proposal on the cybersecurity of the electric sector until and after full implementation;
- To evaluate the cost – *considering an "all hazard approach"* - (direct cost, time, level of expertise) of the implementation of the present proposal for the high- and critical-impact entities, and both association in charge to implement most of the actions (ENTSO-E & DSO Entity).

INTRODUCTION

On 24 May 2023, DG ENER shared a new version of the Network Code for Cybersecurity (henceforth NCCS) for review to the ECG. This review is one of the final steps in the approval of the NCCS. This document provides DSO Entity's comments to the changes made in the DG ENER reviewed version. In preparing these comments, we have in particular analysed whether the NCCS still meets the original goals set out for it.

The NCCS has been under development for many years. Preparations started in 2017 by the Smart Grid Task Force Expert Group 2. They delivered their first draft report in June 2019. These ideas were developed further by an informal TSO and DSO drafting team in 2020, and then by ACER in the framework guidelines published in July 2021. A first proposal for the NCCS was submitted by ENTSO-E and the DSO entity to ACER on 14 January 2022. ACER provided their revision on 6 July 2022.

DSO Entity would like to express its appreciation that the original core objectives for the NCCS are still clearly present in the newest DG ENER revised version. DSO Entity, however, has concern about three of the changes introduced in the latest NCCS version:

- the extension of the scope of the risk assessment to cover non-malicious threats;
- the removal of a requirement to share information from the national entities to entities;
- the change of verification through certification to verification through independent audits.

These changes are deviations from the original elements that have been in the NCCS since the early stages of the multi-stakeholder drafting process. DSO Entity believes that the changes proposed in the latest revised NCCS would impede this Network Code from reaching its original goals. We have, hence, provided recommendations outlined below which would allow to still meet these goals while staying aligned with the NIS2 Directive.

DSO Entity would also like to emphasise the changes in regards of the timelines. Documents developed in the transitional period are made non-binding in the latest revised NCCS version which means that it will take more than 5 years until any of the obligations in the NCCS will become binding. Looking at the changing landscape and the technological advancements, it might decrease the relevance of the proposed harmonised rules of the NCCS. Even though, the NCCS has been drafted to endure resilience, the rapidly changing regulatory and technological environment might strongly affect the gravity of the NCCS requirements. In addition, DSO Entity believes that "we are as strong as our weakest link", thus, as longer as it takes for NCCS requirements to become legally binding, as greater chances we have for uneven distribution in resources and maturity level across Europe. DSO Entity recommends that timelines should be shortened by making the transitional documents into methodologies.

These recommendations are elaborated further below.

LIMIT THE SCOPE OF THE UNION-WIDE AND REGIONAL RISK ASSESSMENTS TO CYBER-ATTACKS

The DG ENER reviewed version of the NCCS extends the scope of the risk assessments and includes non-malicious threats. In the previously proposed NCCS versions (DSO Entity, ENTSO-E and ACER), the Union-wide cybersecurity risk assessment (Article 17) and the Regional cybersecurity risk assessment (Article 19) covered cyber-attacks, defined as any attempt *with malicious intent* to gain access to the network and information systems.

In the latest version proposed by the DG ENER, the scope is extended to cybersecurity incidents, defined as an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems. This extended scope includes non-malicious threats, such as fires, flood, earthquakes, telecommunication outages or power failures.

DSO Entity believes that the scope should be limited to cyber-attacks, because non-malicious threats are covered through other regulations. The Risk preparedness regulation (EU) 2019/941 is already designed to managed natural and accidental hazards. The System Operations Guideline also includes measures to manage risk to the operational security of the electricity system. There would be a large overlap between the NCCS and these other regulations.

The scope of the risk assessment has been restricted to cyber-attacks throughout the drafting process. There have been no objections against this from the Stakeholders. This new approach including “all hazard” risks will have impact on all chapters and concepts developed by the NCCS. The NCCS should probably be considered and written again.

Whilst DSO Entity acknowledges that the EC would like to align the risk management in the NCCS with the all-hazard approach and the definitions in the NIS2 Directive, nevertheless, the Union-wide and Regional risk assessments are processes that are particular to this Network Code. They have no direct equivalent in the NIS2 Directive. The NIS2 Directive already has an all hazard approach when assessing the risk of the affected operators. The NCCS can add value if we also get a union and regional perspective on cyber security incidents. From the point of view of the DSO Entity, it makes sense here to concentrate on malicious cyber incidents, as these can have a direct impact on cross-border power supply and this is the only way we can learn from each other and take countermeasures.

If the extended scope would be kept, more time and effort will be required from scarce experts to perform the risk assessment. Moreover, the extended scope will affect the operational aspects of DSO Entity and the DSOs, thus, a need for increased budget, resources and skillset will be needed which will require time and resilience from the EC and its members.

REQUIRE INFORMATION SHARING FROM NATIONAL AGENCIES TO ENTITIES

The DG ENER proposed version of the NCCS removes the requirement for the national competent authorities to share information on incidents with the high impact and critical impact entities[1]. In the ACER version, information on reportable incidents were shared in three steps:

1. Entities report incidents to the competent authorities in their Member States;
2. The competent authorities share an anonymise & sanitize report of the incident with all national single points of contact under the NIS2 Directive, through the national CSIRT;
3. Each competent authority in each Member State share this information received to the high- and critical-impact entities in their Member State.

The last step has been removed in the latest version[2]. Consequently, information on incidents may not reach entities in other Members States.

DSO Entity believes that the NCCS should include an obligation to inform high-impact and critical-impact entities about incident that could occur in their system and could have an impact on their cybersecurity in order to organize their operational defence against cyber threats.

The NIS2 Directive allows national CSIRTs to share incident information but it does not require them to do so which might result in ineffective and imbalanced communication National agencies need to set up processes and systems in order to rapidly share the information. They might consider certain information as too confidential. To overcome these barriers, it is important to have a legal obligation that requires timely information sharing.

As a Delegated Act, the NCCS may not be able to place new requirements on national CSIRTs or national single points of contacts defined under the NIS2 Directive, nevertheless, the requirement to foster this communication should be added.

If no requirement for sharing with entities is included, there is a risk that important incident information will not reach the entities or will reach them too late to be of practical use. This would undermine the main goal of information sharing - helping these entities to quickly respond to cyberattacks.

[1] *Art.40 (1)(e) in the ACER's version dated July 6, 2022*
[2] *Art.37(1) of the latest version shared by the European Commission*

INCLUDE QUALITY REQUIREMENTS ON INDEPENDENT AUDITS

The DG ENER revised version replaces the option of verification through certification by verification through independent audits. In the ACER proposed NCCS version, there were three options for an entity to provide verification evidence of the management system and cybersecurity controls:

- Being certified or audited by an independent conformity assessment body;
- Through peer reviews;
- Through inspection by the competent authority.

In the DG ENER reviewed version, the first option is replaced by 'undergoing independent security audits.

DSO Entity believes that the NCCS should include quality requirements on how the independent audits are being performed. If audits are performed by a conformity assessment body, such quality requirements should be enforced through accreditation. The national accreditation bodies, for instance, ensures that audits are performed by qualified staff and that there is a minimum number of auditing days.

Quality requirements for audits are already included in the NCCS for the other two verification options (peer reviews and inspection by the competent authority) in Article 23(2). This article requires that:

- Parties performing audits are independent and have no conflicts of interest.
- Auditors have demonstrable knowledge of relevant security topics.
- Auditors have sufficient time to perform the audit.
- Confidential information from the audits is protected.
- Audits are performed periodically.

DSO Entity would like to propose to make the requirements in Article 23(2) also applicable to verification by undergoing independent audits.

If no quality requirements are included for the audits, it can be expected that there might be large differences between how strict the audits are being performed between various Member States and entities. This would mean that a consistent baseline would not be reached for security throughout the European electricity system. Reaching such a baseline was one of the main, original goals of the NCCS. Such a common baseline is crucial as all entities in a region are connected to the same electricity system and attackers will be looking for the weakest spot to disrupt it.

MAKE THE TRANSITIONAL DOCUMENTS BINDING

In the DG ENER reviewed version of the NCCS, the documents developed in the transitional period are made non-binding. It concerns three documents (Article 48(1)):

- A transitional electricity cybersecurity impact index (ECII);
- A transitional list of Union-wide high-impact and critical impact processes;
- A transitional list of European and international standards and controls required by national legislation with relevance for cybersecurity aspects of cross-border electricity flows.

Currently all these documents are non-binding, thus, it will require 63 months (more than 5 years) after entry into force before any of the provisions of this Network Code will become binding.

DSO Entity believes that the transitional documents need to be made binding by turning them into methodologies that are approved according to the process in Article 7 of the NCCS. If the documents are approved in this way, the competent authorities can use them to identify high-impact and critical-impact entities much earlier.

There are two drawbacks to making the transitional documents binding for the most critical entities[3]:

- The approval by the competent authorities will take time. The approval can however still fit into the transitional period. If proposals for the documents are submitted by the TSOs & DSOs 6 months after entry into force, this would leave 18 months for the approval process and for the competent authorities to identify the high-impact and critical-impact entities.
- The documents are not based on the Union-wide and regional cybersecurity risk assessments. There is not enough time to perform these risk assessments before the documents need to be submitted. This issue can be addressed by using the pre-cautionary principle - only identify entities as high-impact or critical-impact if they are sure to affect the operational security of the grid and only select controls from the standards if these are clearly needed for risk mitigation.

DSO Entity believes that these drawbacks are clearly outweighed by the benefits.

If the transitional documents are kept as non-binding, competent authorities can only start identifying high-impact and critical-impact entities after they have been notified of the Union-wide cybersecurity risk assessment report, 54 months after entry into force of the NCCS. The identified entities would then be notified 9 months later, 63 months after entry into force. They have to implement the minimum and advanced cybersecurity controls 12 months after notification (75 months after entry into force) and provide verification evidence 24 months after notification (87 months after entry into force). To sum up, it takes more than seven years before the obligations in the NCCS need to be fulfilled by entities. DSO Entity strongly believes that the proposed timeline will affect Europe`s ability to respond to cybersecurity threats to the electricity systems.

[3] *During the last discussion between ENTSO-E & DSO Entity experts, it seems obvious that the entities dealing with more than 3GW would be considered as critical.*

REMOVE THE ARTICLE ON SECURITY MEASURES FOR CRITICAL SERVICE PROVIDERS

The DG ENER reviewed version transfers the obligations from critical service providers to the entities. In the previous version, the task of the critical service providers was to implement three types of requirements:

- Secure design, development and production;
- Vulnerability management;
- Protection of assets and information.

In the new version, entities are now required to ensure that their critical suppliers meet these requirements in Article 32.

ENTSO-E therefore recommends removing this article and consider the security measures for critical service providers to be covered by the supply chain security controls required by Article 31. These controls will already require high- and critical-impact entities to set security requirements to their suppliers, and to ensure these are fulfilled through monitoring, reviewing and auditing the supplier.

Article 32 just repeats measures already covered by Article 31. Secure design, development and production (Article 32(1)) is covered by Article 31(a)(ii). Vulnerability management (Article 32(2)) is covered by Article 31(a)(vii). Protection of assets and information is covered by Article 31(a)(iv).

Article 31 works together with other elements in the network code and ensure that the measures for suppliers are implemented well. It provides a link of the measures to the risk assessments. And it defines how entities should ensure that suppliers implement measures through the minimum and advanced cybersecurity controls. The management system and verification can then be used to make sure that the controls are implemented at the entity. Article 32 is not linked to the other mechanisms in the network code at all.

The Cyber Resilience Act (CRA) will also cover many of the requirement in Article 32. ENTSO-E believes that supply chain security risks are already exhaustively regulated through Article 31 on the entity side and the CRA on the supplier side. Adding additional requirements in Article 32 seems to lead to overregulation.

If the security measures for critical service providers in Article 32 are kept, this will pose many practical problems for both entities and critical service providers. It is not clear how far entities should go to ensure that the supplier has implemented the measures. If each entity starts doing audits or assessments on all their critical providers, this will likely create capacity problems at auditors and suppliers. Moreover, not all existing contracts will include a right to audit. And it is not clear what an entity can do if their supplier is not providing the information needed to ensure implementation of measures.