Government Offices of Sweden

Memorandum

10 December 2021

Ministry of Infrastructure
Energy Division, Energy Division
Departementssekreterare
Katarina Yuen
katarina.yuen@regeringskansliet.se

ENTSO-E Operations Team
Daiga Dege
daiga.dege@entsoe.eu

Response to ENTSO-E consultation of draft of network code on cybersecurity (NCCS)

Our society depends on the function of the electricity system, and for the decarbonisation that is needed, the electricity system needs to evolve. As it does, it is becoming more dependent on operational technology and data exchange between more and more participants. The European electricity system is integrated, and the internal electricity market is essential to the value chain delivering electricity to all Europeans. In this context cybersecurity is critical, and as the electricity system is interconnected throughout Europe, harmonised cybersecurity efforts will allow for better cooperation and a more even playing field for market participants. The Swedish Government welcomes the ongoing work with legal acts promoting cybersecurity. We appreciate this opportunity to address some concerns regarding the network code on cybersecurity.

First, some general issues are addressed regarding harmonisation with other legislation, scope, roles of authorities and national security. Following that, more specific comments are given related to some of the articles in the draft. The comments given here may pertain to issues that are included in the non-binding framework guideline and that the drafting committee is not entirely at liberty to address in the drafted legal text. However, in a response to comments, the committee may provide explanations.

A full analysis of the legal text has not been made at this stage in the drafting process, and further analysis and opportunity to comment will be necessary.

1. Harmonisation with NIS/NIS2 and other EU regulation

Directive 2016/1148 (NIS) and the proposal for a new NIS directive (NIS2) have been used relating to some existing functions, definitions, etc. It is unfortunate that the timing in the development of the NIS2 and NCCS does not allow for their harmonisation, and we would urge for some consideration in the adoption of NCCS so that greater harmonisation is possible. The cost for not doing so will be borne by entities and authorities alike, all actors with limited resources and already putting much effort into the development of the electricity system. A cost benefit analysis of the requirements should be performed. The goal is of course increased cybersecurity, not increased requirements.

SE views NIS/NIS2 as overarching legislation setting a baseline for cybersecurity within the union to ensure the functionality of necessary societal functions which to a large extent are integrated with the internal market. A sector-specific act such as the NCCS should use existing legislation as a starting point and thereafter complement it by providing *additional* requirements necessary for the function of cross-border electricity flows. An alternative approach is to view the NCCS as sector-specific legislation with requirements of at least equivalent effect to the obligations laid down in NIS/NIS2. Such an approach requires further guidance pertaining to any differences between the goals of each act, identification of entities and subsequent requirements in the respective acts, as well as coordination between risk assessment processes in order to provide coherent risk assessments at relevant levels without duplication.

Establishing a clear relationship between NIS/NIS2 and NCCS is fundamental in understanding the relevant scope for each act, both in terms of *whom* is concerned and *what* is required. Viewing the NCCS as a complement to baseline cybersecurity legislation stemming from NIS/NIS2 one might expect it to relate to core business processes in the internal electricity market, such as those facilitated by RCCs, thus targeting a smaller scope. Viewing NCCS as a sector-specific act to replace requirements in NIS/NIS2 one might expect it to target a broader scope, but the NIS/NIS2 requirements that thus become redundant must be clearly identified.

Article 3(2)(f) of the draft states that double reporting and additional administrative burdens should be avoided, but how this is to be done in relation to NIS2 is not clarified. While not yet finalised or implemented in

national legislation, the draft NIS2 and NCCS give an impression of similar, parallel efforts to be put forth by to a large extent the same actors, and reporting to be made to not quite the same set of authorities.

Relevant procurement requirements play an important role in cybersecurity. However, requirements need to be developed in light of other regulations. Sector specific requirements or standards will contribute to a fragmentation within cyber- and information security which may result in inefficient security efforts as requirements are effectively doubled or possibly contradictory.

With other regulation and existing standards as a starting point, the scope of the NCCS will become clearer, and the legal text possibly much simplified.

2. Roles of authorities and other bodies

Roles of authorities and bodies have been established within NIS legislation to promote cybersecurity, and within electricity market legislation to promote electricity market efficiency. Both sets of authorities and bodies (on European and at national levels) are addressed and given extensive roles in the NCCS.

While the involvement of bodies resulting from cybersecurity legislation is appreciated for the sake of coordination, the mandate for the network code to require their action is unclear. Furthermore, by involving both sides extensively, information will be shared more often, resulting in increased risks when sharing sensitive information, the risk of duplication of work efforts, need for duplication of cybersecurity competence at authorities, and uncertainty for entities as to which authority to look to. The relationship between NIS/NIS2 and NCCS is also fundamental in understanding how concerned authorities should relate to each other.

The implementation of CS-NCA in different member states may vary. The current implementation in Sweden is one competent authority and several sector-specific regulatory authorities within cybersecurity. Sector-specific authorities are however better equipped to understand the specific roles and processes within the sector.

The purpose and efficiency of setting requirements on different authorities in the NCCS should be described in a way that clearly explains areas of

responsibility, the need for multiple roles, and how they should interact or relate to other functions. Allowing for national designation of the relevant authorities should be possible.

3. National security of member states and information exchange

The purpose of the NCCS is to increase security related to cross-border electricity flows. All exchange of information required by the NCCS needs to be decided in light of this purpose so that the risks that are introduced by sharing information are outweighed by benefits, resulting in an overall reduction of security risks. Which information is shared, which entities that have access to information, and aggregation of information need to be considered carefully.

National security is the sole responsibility of each member state (article 4(2) Treaty on European Union, TEU), and the network code must allow for this. No member state shall be obliged to supply information the disclosure of which it considers to be contrary to the essential interests of its security (article 346 Treaty on the Functioning of the European Union, TFEU). In article 3 of the NCCS draft, respect for national legislation is mentioned but should for national security issues be explicit. Texts should be aligned with the NIS2 and consequently also make it clear that the exemption for the purpose of national security applies regardless of which entity is carrying out those activities and whether it is a public entity or a private entity.

It should be assumed that a significant part of the reporting described in the NCCS will include classified information. We take it for granted that all such handling of classified information should be covered by the Council Security Rules (CSR) or equivalent requirements. If classified information is handled this will also, in accordance with the CSR, require the use of approved products for transmission and handling of information. Planning for such infrastructure must be initiated in a timely manner.

4. Timeframes

It is apparent from the draft and the consultation questions that implementation time frames have been considered and that there is an interest in setting consistent and realistic time frames. For concerned electricity system actors and authorities, understanding the scope of requirements and timeframes is essential for effective planning of personnel, means for handling and sharing of potentially classified information, etc. The

timeframes and deadlines, and their interdependencies, are not all easily discerned in the draft.

Regular updates to risk assessments is important, and a 2-year cycle may be appropriate. Some of the processes described in the draft use a 3-year cycle. The relation between these time cycles should be considered.

5. Comments to articles

This section contains more specific comments relating to some articles.

5.1 Article 2 Scope

Overall, the scope of NCCS depends, or should depend, on how it relates to NIS/NIS2.

Several of the existing network codes and guidelines use various methods and characteristics to identify contextually relevant assets and actors. For example, the identification of Significant Grid Users (SGU), Critical Network Elements, Observational area and Relevant Assets for Outage Coordination as established in regulations 2015/122, 2017/1485 and 2017/2196. As the identification relates to cross-border electricity flows in these acts, as well as in NCCS, a similar approach could be useful.

The risk-based approach applied later in the draft is appreciated, as well as the possibility of including smaller sized entities if relevant. However, this also makes it difficult for smaller entities to determine whether they are included. Regarding article 2(2), are the conditions in (a) and (b) both required as indicated in the last paragraph ("*and other entity that fulfil the conditions 2(a) and 2(b).*")?

The reference to article 2(1) as used in several places in the draft could be reviewed. All entities listed in article 2(1) is understood as all entities listed in 2(1), irrespective of if they are included in 2(2) or anywhere else. Later the terms *critical-impact* and *high-impact* entities are established and used. These are in some sense analogue to terms such as SGU and any possible harmonisation is likely to be helpful in the application and monitoring of legal acts.

In article 2(3) the removal of a word may be necessary so that not all entities outside the scope of the network code are targeted: "…*and any other entity ~~not~~ listed in Article 2(1), not classified as*…".

5.2 Article 3 Objectives

Objectives could be related to the overall objectives provided: rules on common minimum requirements, planning, monitoring, reporting and crisis management. While many detailed objectives may give some clarity, they may also obstruct overall intentions.

Conflicts with national security and duplication of requirements in relation to other EU legislation need to be addressed, as commented above.

5.3 Article 4 Definitions

Each definition needs to be very carefully considered, both regarding the necessity of the definition and the exact wording. Definitions existing in other legal acts should not be replicated. This is, as understood by the supporting document, not intended for the final draft.

Some definitions are very similar to, but not exactly the same as existing definitions, and it is not clear if a new term is introduced, and if it is necessary for example, *cross-border electricity flows* vs. *cross-border flows*.

In other instances, terms are used in other articles that differ from the definitions in article 4, for example the term *competent regulatory authority* is used multiple times and it is not clear which authority is intended.

Some sets of terms are defined with perhaps excessive detail, while others lack in detail. For example, *critical* and *high impact entities* are defined through a sequence of definitions, but also determined explicitly in a process in a later article. *Critical service providers* are simply providers of critical services.

The definition of *critical-impact electricity crisis* is very similar to the definition of *electricity crisis* as in regulation 2019/941. The definition of *cross-border electricity crisis* is very similar to the definition of *simultaneous electricity crisis* in regulation 2019/941. In Title VIII the term *cybersecurity crisis* is used. Electricity crises relate to electricity shortage or inability to supply electricity, which are quite grave situations. More nuances are perhaps found in the *system states* as defined in regulation 2017/1485. As the proper functioning of tools and

facilities is included in the criteria for determining system state, this may be a useful term also in the NCCS.

Definitions should be aligned with NIS2 and CER.

5.4 Article 5 Methodologies

The usage of methodologies in order to implement details and allow for more frequent adjustments may be effective. Such an approach could motivate a lower degree of detail in the underlying act.

The methodologies listed in article 5(4) are not all presented as methodologies later in the texts. Article 17(1) provides a clear set of methodologies to be produced within a given time frame and to be applied according to other articles. Several other listed "methodologies" refer to "reports" and it is unclear if the approval mentioned in article 5 relates to each biannual report or a method to be followed when producing the report.

The terms *all competent regulatory authorities* and *the competent regulatory authority* are used in several places. It is not clear which authorities are intended. In Article 5(7) it is unclear what is meant by competent in the phrase "*Regulatory authorities or, where competent, ACER*".

The reference in article 5(5)(a) to article 20 should perhaps be to article 21.

5.5 Article 6 Publication of methodologies on the internet

The term *competent NRAs* is unclear.

The necessity of article 6(2) is unclear.

5.6 Article 10, 11, 46 Confidentiality and information classification

Terminology should be harmonised and aligned with existing EU terminology.

Classified information should not be disclosed by member states if doing so is considered to be in conflict with national security interests.

5.7 Article 12 Monitoring

The allocation of responsibilities amongst ACER and the monitoring body should be further clarified. What are the expectations of the monitoring

body and is the intention to have the monitoring body assisting ACER with the monitoring? What is the benefit of establishing a monitoring body compared with other alternatives, e.g. that ACER should monitor implementation and in this context confer with other relevant bodies?

Why does the monitoring refer to the objectives in the "Joint communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade" rather than the objectives in article 3?

Regarding article 12(3), what is the difference between methodology and rules? The set of information requested as well as the means of communication and access to information should be subject to the assessment of member states or relevant security authorities regarding the sensitivity of information in relation to national security. The value of providing information and the necessity for each entity able to access the information needs to be clear.

5.8 Article 13 Benchmarking

The objective of the benchmarking and how the results could be used should be specified. For example, what is the expected impact of performing the benchmarking? What type of method will be used for the benchmarking, and will it be similar for all member states? Separating security costs from other investment and operations costs may not be possible in all instances.

In paragraph (4) CS-NRA should perhaps be CS-NCA.

5.9 Article 14 Agreements with TSOs and DSOs not bound by this Regulation

The consequence of including a deadline that cannot be enforced is unclear.

5.10 Article 20 and 21 Regional cybersecurity risks

It is not clear from these articles and article 5(5) if regulatory authorities approve risk treatment plans every two years or a methodology for performing risk assessments. Thresholds for acceptable residual risks could be established in a methodology.

Additional tasks assigned to the RCCs may need to be considered according to article 37(2) of the electricity marked regulation (2019/943).

5.11 Article 23, 24 and 25 Cybersecurity framework

The timeframe for development of the framework is not clear. The details are not set out in the legal text. Rather, the framework of controls/measures is to be developed. This may be a rational approach as it allows for more flexibility and more gradual learning to be incorporated. It does however also introduce much uncertainty as to the scope and level of detail to be expected, which adds to the overall uncertainty regarding requirements in the NCCS as well as its effectiveness.

While it is reasonable to set cybersecurity procurement requirements based on the results of the cybersecurity risk assessment at entity level, it is important to define the requirements without compromising competitiveness amongst suppliers of ICT products, services or processes. Existing European cybersecurity certification should be used as a starting point. Sector specific standards risk fragmenting cybersecurity.

5.12 Article 26 Member State cybersecurity risk assessment

Although the methodology is not yet developed, performing a risk assessment on all high-impact and critical-impact entities within a Member State appears a significant task. The business processes that are high and critical impact are likely to include such business processes as those developed pertaining to other network codes and guidelines. CS-NCAs may not be particularly familiar with these. In the provision of data, both to and from the CS-NCA, relevant information security needs to be ensured. The costs, both in terms of required resources and increases security risks, need to be in proportion to the enhanced cybersecurity.

The time frame in article 26(3) should be 9 months in order to be in harmony with 26(2) and 31(2).

5.13 Article 27 Identification of high-impact and critical-impact entities

When an explicit list of entities is produced and shared the need for doing so must be clear. The value added by collecting such lists at ENTSO-E and the EU DSO entity is not clear and security risks of such aggregated information must be considered. The creation and maintenance of such lists requires administrative costs.

The transitional list to be produces according to article 49 is to be published on websites. The risk and value of this is not clear.

5.14 Article 29 and 31 Risk assessment at entity level

Article 29(5) states that entities shall report the controls it implements for risk treatment to its NRA and its CS-NCA. In article 31(1)(a) it is stated that a *summary* of threats, existing controls and vulnerabilities shall be provided to the CS-NCA. The two are not aligned in this sense, and the value of reporting each control is not clear.

5.15 Article 30 Derogations from the minimum and advanced cybersecurity controls

While allowing derogations is reasonable, it should be clearly stated on what basis the derogations can be made and in what time frame. In order to provide derogations given that the requirements in (a)-(c) are met, details and methodology on how the assessment should be performed should be clarified.

Article 30(1) is not understood as a derogation.

5.16 Title VII Harmonised cybersecurity procurement requirements

As noted earlier, requirements need to be developed in light of other regulations and standards. The need for sector specific requirements is not made clear, however the need should be made clear before such requirements are established.

This section should be thoroughly aligned with Title IV.

5.17 Title VIII Essential information flows, incident and crisis management

Incident and crisis management that relies on existing bodies such as CSIRT and ENISA should also rely on existing processes in these bodies except for where there are specific needs within the sector.

Cybersecurity crises for the electricity sector are not defined. Electricity crises are defined through regulation 2019/941 (RP) and in this context the root cause of the electricity crisis can be related to cybersecurity. Since crisis management planning also is included in RP, this should not be duplicated.

The title includes "essential information flows". Is this to be understood as information flows that are essential in crisis management or essential to cross-border electricity flows? A significant amount of information exchange

is required in the draft that is not mentioned in this title, and thus not included in article 48 Protection of information exchanged in the context of Title VIII.

The consequence of 3-year cycles for plans versus 2-year cycles for risk assessments should be considered. Six months may be more easily applied than 180 days.

From article 42 it is interpreted that the early warning capabilities (ECEWC) is perhaps a platform for information exchange and a function which should analyse and disseminate information and suggestions. The introduction of further communication platforms should be avoided. Rather, existing platforms should be used.

5.18 Title IX Electricity cybersecurity exercise framework

Exercises can be very helpful in learning processes and is a welcome component. Cybersecurity is however one of several risk and preparedness areas that the electricity sector faces and the possibility to combine cybersecurity exercises with other exercises within sector should be considered.

The development of exercises at a national level should be given more flexibility in order to involve appropriate authorities and coordinate synergies with other exercises. Once again, the scope and relationship to NIS/NIS2 is important in understanding the work entailed by this title.

5.19 Title X Protection of information exchanged in the context of this data processing

It is not clear what *this data processing* in the title refers to.

Various types of information exchange are required by the draft relating to identifying entities and processes, risk assessments, monitoring, etc. And at the core of the business processes that are integral to cross-border electricity flows lies an extensive data exchange. This is not entirely reflected in title X, at least not in the sense that title VIII seems to be limited to information exchange related to crisis management.

5.20 Article 49 Transitional provisions

Article 49(3) requires the establishment of lists of high and critical impact entities, that these lists should be aggregated and published on websites. The purpose of this is not clear, and the risks involved with this type of information handling are not managed. Is the same treatment of the lists required in the regular cycles?

5.21 Annex A Basic cybersecurity hygiene requirements

The cybersecurity hygiene requirements are seemingly not advanced. However, several could be clarified. For example, what should an incident response plan include and what are the criteria to approve the plan? How often should data be backed up? And what does it entail to manage data?

Considering the uncertainty in what the requirements entail, the implementation time frame of twelve months, stated in Article 2 (1), could somewhat short.