INSTITUT LUXEMBOURGEOIS
DE RÉGULATION

Luxembourg, the 10th of December 2021

ENTSO-E and EU.DSO
Rue de Spa 8
B-1000 Brussels

Reference CH/CHO/SB/ffr ILR21007705

Contact Fréderic-Michael Foeteler – T +352 28228 347 – e-mail: frederic-michael.foeteler@ilr.lu

Subject Network Code for Cybersecurity aspects of cross-border electricity flows.
Contribution of the Institut Luxembourgeois de Régulation with regard to the public consultation process.

Dear Ladies and Gentlemen,

please find hereafter a list of concerns and comments in relation to the above-mentioned ongoing public consultation[1].

We would be happy if you would take these considerations into account for the further development of the Network Code for Cybersecurity aspects of cross-border electricity flows (hereafter referred to as "NCCS") and we look forward in providing you any further information you might require.

On behalf of the Institut Luxembourgeois de Régulation

Camille Hierzig
Directeur adjoint

Attached: ILR contribution with regard to the public consultation process for the NCCS.

17, rue du Fossé
Adresse postale
L-2922 Luxembourg

T +352 28 228 228
F +352 28 228 229
info@ilr.lu

www.ilr.lu

[1] A copy of the present letter is being sent to the Luxembourg Ministry of Energy and Spatial Planning and to Creos Luxembourg s.a. in its capacity as Transport Systems Operator for the electricity market.

Applicability

Article 2 (2) states that *"This Regulation shall not apply to a micro or small sized enterprise, or any other entity not listed in Article 2 (1)..."*.

However, the term "micro or small sized enterprise" is not defined in this regulation; in the absence of a common definition, it should therefore be left to each Member State or to the relevant authorities to decide which company has to submit to the rules of the NCCS.

Electricity entity

The present text of the NCCS defines various organizations as "electricity entity", including the NRAs and the CS-NCAs. We believe however that the roles of the NRA and of the CS-NCA must be clearly distinguished from those of the operational market actors (grid operators, energy suppliers…) and that their different tasks and responsibilities should be more accurately stated in the text of the NCCS.

Competencies and duties of the individual actors

In numerous places the document contains indications that the NRA and the CS-NCA have to decide or do something together (*"the CS-NCA and the NRA decide"*, *"the CS-NCA and the NRA shall report"* etc.).

We believe that the respective roles of both institutions in relation to the NCCS should be clearly defined in order to avoid misunderstandings regarding the competences and responsibilities of both actors.

If the authors of the document prefer to leave it to the individual Member State to regulate these responsibilities, this should also be clearly defined in the NCCS.

In that case, it could be decided, for example, that each MS decides for itself whether either the NRA or the CS-NCA takes over the coordination of all activities with regard to the national implementation and the subsequent monitoring of the rules and commits itself accordingly to the other respective authority to align upon the division / coordination of tasks.

In analogy hereto, it is not clear how ENTSO-E and the EU DSO entity will share their tasks and what the relevant communication channels from and towards them should look like.

The current version of the NCCS and its supporting document do address the difficulty, but a satisfying answer is not given. To make sure the individual organizations (e.g. ACER, ENISA, ENTSO-E, EU DSO entity, RCC, NEMOs, NRAs, RP-NCAs, CS-NCAs, CSIRTs and, not to forget, TSOs and DSOs) will - in the years to come - not get lost in competence disputes, it would be helpful if the NCCS early on defines clear hierarchies and communication channels.

Also the overall calendar of assessments could be structured in a more comprehensive manner.

Comparable set of rules for NCSS and NIS Directive[2]

In the context of the NIS Directive, regular reports regarding incidents related to cybersecurity must be submitted by an electricity undertaking to the CS-NCA.

As with regard to the NCCS however, only incidents related to cross-border electricity transmission need to be documented.

In order not to unnecessarily burden the organization of an electricity undertaking, especially in critical moments, the form of reporting should be as identical as possible in both cases, i.e. the content of the information to be transmitted, the format, the communication channels and the

[2] "NIS Directive" or "NIS" means the "EU Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union" whereas its successor version is hereafter referred to as "NISD2".

ILR
INSTITUT
LUXEMBOURGEOIS
DE RÉGULATION

17, rue du Fossé
Adresse postale
L-2922 Luxembourg

T +352 28 228 228
F +352 28 228 229
info@ilr.lu

www.ilr.lu

deadlines should be uniform between the NCCS and the NIS Directive. Further to this, double reporting (NCSS & NIS) should be avoided wherever possible.

Role of CSIRTs/CERTs in case of a cyber-incident

As with regard to the phrase in Article 37 (4) "*In the event of a cyber-incident or cyber-attack, the CS-NCA or the CSIRT shall assess the level of classification of the information received from the entity and shall inform the entity about the outcome of its assessment within eighteen (18) hours of receipt of the information*", it is our belief that a Member State's CSIRT is usually unable to process cyber incidents with different classifications and within different time limits, depending on whether the incident is in the electricity sector or in another area.
So in any case, one should pay attention to ensure that the responsibilities and deadlines defined in the NCCS are always compatible with those in the NIS/NISD2.

The definition of CSIRTs / CERTs in Article 37 (5) (d) is not compatible with the mission of CERTs.
The text makes undue abstraction of the complexity of the handling "vulnerabilities such as 0 day vulnerabilities".
For CERTs, the protection of their constituency is of paramount importance; CERTs are bound to inform their constituents when there is knowledge of a vulnerability, this to allow them to put in place alternative protection mechanisms until the "vendor" provides a patch "or other mitigation measures" which can be a troublesome and lengthy process.
As a matter of fact, when considering the behaviour of vendors, it is not always primarily driven by the interest of their clients nor of the one of cybersecurity. Many examples exist in that regard, for instance the events around the Tanium meltdown of the Microsoft exchange servers in March 2021; there was undue delay and even suppression of information and mitigation measures by Microsoft on git.
Therefore, the ILR, in orchestration with the Luxembourg CERT[3], proposes to rephrase the bespoken Article 37 (5) (d) into "not share vulnerabilities such as 0 day vulnerabilities not publicly known outside of their peer network and the constituency on a need to know basis (under TLP red?). The vendor shall provide all the information necessary for a containment of the incident until the patch or other workable mitigation measures to the concerned entity are available;".

Crisis management

The responsibilities defined in Article 40 need to be better formulated in order to avoid possible misunderstandings as far as possible.
The way in which crises are to be dealt with and who has what responsibilities are defined differently in the individual Member States and crisis management is not automatically a matter of the CS-NCA, but may be subject to other authorities in other countries.
For this reason we recommend introducing the wording in Article 40 (1) as follows: "Unless otherwise defined by the Member State, the responsibility for crisis management in the event of a cyber-incident related to the cross-border electricity flows rests with the CS-NCA…".

Link with the Risk-Preparedness Regulation 2019/941 and its provisions

It should be ensured that the risk assessments and the crisis management are consistent with the provisions in the risk preparedness plans which also consider cybersecurity as a high risk scenario, and that there is no double work on this matter. This notably concerns Article 17, Title III (Articles 19 to 22), Title V (Article 26), and the Articles 44 to 45.
A link with the risk-preparedness regulation 2019/941 should be mentioned in the NCCS.
In addition, Article 43 needs to ensure a consistent process with the cybersecurity exercise already defined in national plans when a NRA is assigned to perform such exercise.
It is furthermore essential that the requirements with regard to the content and the form of the risk assessment largely correspond to the expectations of the risk assessment that the relevant actors must submit to the CS-NCA in the context of NISD2.

[3] https://www.govcert.lu/en

ILR
INSTITUT LUXEMBOURGEOIS DE RÉGULATION
17, rue du Fossé
Adresse postale
L-2922 Luxembourg
T +352 28 228 228
F +352 28 228 229
info@ilr.lu
www.ilr.lu

Deadlines
The document specifies binding deadlines for how often cybersecurity exercises and risk assessments must be carried out. We believe that instead of writing *"every X years"*, it would be better to define "at least every X years" as a guideline.

Certification scope
It is not clear from the text whether an electricity undertaking, whose role is considered as "critical" must be certified in its entire organization or whether the certification obligation can be limited to that part of the company, whose activity potentially has a cross border impact.
If an entire organisation has to be certified, a period of 2 years seems rather short.

Adoption of methodologies
In general, the procedures highlighted in Article 5 are not consistent in all their aspects, in particular regarding the all NRA approval procedure at regional level (no individual NRA approval procedure is foreseen under this Regulation by Article 5(5)) and should be reviewed accordingly.

Service Suppliers
To what extent is there an obligation to require service suppliers, who play an important role in the supply chain of an electricity undertaking, to adhere the rules specified in the NCCS?

For instance the service supplier of a SCADA system plays an important role for the grid operator, as he regularly improves the software he sold to its customer and applies these changes on the productive system of the grid operator by means of software or parameter updates via remote maintenance (under the condition that the grid operator gave its upfront consent).
The service supplier does not take any decision regarding the operational use of his software, but could theoretically change the productive system through incorrect remote maintenance (e.g. due to defective software or incorrect parameterization) so that it leads - directly or indirectly - to undesirable behaviour.

The final responsibility always remains with the grid operator and it seems difficult to implement obligations towards an external service supplier to submit to the same rules as the operator itself. This aspect should be further clarified in the document.

Critical services
It is stated that *"this Regulation shall apply to critical service providers"* and that *"critical service provider means a natural or legal person who operates or provides any critical service directly or on behalf of an entity"*.
Who defines what a "critical service" is?
Is this at the discretion of the CS-NCA or will a general guideline be drawn up in that regard?

Bugs
What about incidents that are indeed IT problems, but which are not the result of malicious manipulation but caused by faulty software?
Must such incidents also be treated as cybersecurity incidents according to the rules described in the NCCS and within the same delays?

ILR
INSTITUT
LUXEMBOURGEOIS
DE RÉGULATION

17, rue du Fossé
Adresse postale
L-2922 Luxembourg

T +352 28 228 228
F +352 28 228 229
info@ilr.lu

www.ilr.lu

Annex A – Basic Cybersecurity hygiene requirements
The requirements formulated in Annex A for smaller actors that are not directly affected by the NCCS are defined unfavourably.

The set of rules should be written in such a way that it remains valid and meaningful over a long period of time without its content having to be regularly adapted to the (often rapidly changing) technical circumstances.

This means that the list of the nine minimum requirements should either be described more generally or the document could refer to existing (or yet to be written) general recommendations from ENISA, which in turn would contain generally applicable technical and organizational recommendations that would to be adapted over time as technology evolves.

Editorial remarks
The supporting document[4] contains eight errors with regard to misplaced hyperlinks, which is not helpful. Further to this, the numbering of the illustrations in the document is incomplete and inconsistent; the second illustration in chapter 12 is illegible.

Deadlines
We believe that the deadlines are too tight and that it will be very difficult, if not impossible, to publish the text of the NCCS on time.
Given the many imperfections in the text, we doubt that a revision can be done within the foreseen delays.
In our opinion, it would be advisable to extend the relevant deadlines by 3 months.

ILR
INSTITUT
LUXEMBOURGEOIS
DE RÉGULATION

17, rue du Fossé
Adresse postale
L-2922 Luxembourg

T +352 28 228 228
F +352 28 228 229
info@ilr.lu

www.ilr.lu

[4] See "211112_NCCS_Supporting Document for Public Consultation.pdf".