**NETWORK CODE ON CYBERSECURITY**

**WORKSHOP**

**Microsoft Teams**

**19th November from 14:00 to 17:00**

**Q&A**

***Question: What minimum and advanced requirements the Network Code on Cybersecurity will specifically contain? Will other elements be added (Art. 23)?***

Answer: First, we need to identify what are the critical entities and processes and, afterwards, specific controls / requirements will be developed by ENTSO-E and the EU DSO entity together with the stakeholders.

***Question: Some flexibility is needed. Is it possible to frame what requirements could come? Where these requirements are mentioned - in Article 21 and 23? Currently the requirements are mentioned in several parts of the document. Would the procedures be different, and would they be subject to regulatory approval?***

Answer: The procedure of Article 5 of the Network Code will be followed to develop the minimum and advanced controls (Art. 23). The minimum and advances controls will include controls for the supply chain security (Art. 24). The regional cybersecurity risk treatment plans shall list the respective controls (Art. 21).

The process to assess which controls apply to which entity / perimeter would be as follows - identify critical business processes and assess them, then link them with the risks. It is important to note that the strictest security controls will apply to the highest risks.

***Question: Should a regulator supervise itself? This question refers to Article 2 (minimum provisions that apply to entities and regulators).***

Answer: ACER will monitor how the Network Code provisions are implemented.

**Question: Member States cannot appoint CSIRTs, why is this referred to in Article 9 of Directive (EU) 2016/1148?**

Answer: CSIRTs designation is set out in the NIS Directive; the Network Code on Cybersecurity does not duplicate already existing legally binding rules.

***Comment: The benchmarking approach (Art. 13) refers to expenditure, these costs are very different in various regions in Europe, therefore, it will be very difficult to compare them. It would be recommended to add a description on how the expenditures could be compared.***

***Comment: Regarding the benchmarking (Art. 13), it is very difficult to compare expenditures for cybersecurity because it is not known what part cybersecurity measures represents in different IT solutions. Efficient cyber protection should not be measured against the costs.***

***Question: Financial damage should be considered in the risk assessment (Art. 19 and Art. 26). What is your position on this matter?***

Answer: We do not consider financial damages, because the Network Code on Cybersecurity aims only at cross-border operational controls. For the same reason, public image damage is not taken into account.

***Question: Is it possible to link cybersecurity controls to existing cybersecurity requirements/standards?***

Answer: A mapping exercise will be done in the future (Art. 25). During this process, we will try to map all relevant national regulations and international standards.

***Question: There will be a working group (Art. 15) with a lot of powers, and it will provide major deliverables. ENTSO-E and EU DSO will mainly oversee these deliverables. Would it be possible for stakeholders to intervene on who would be the best to implement these deliverables? Why not use the ENTSO-E Stakeholder Committee for this task?***

Answer: Broad stakeholders involvement is foreseen in the Network Code on Cybersecurity via the Working Group and the public consultation to develop these deliverables (Art. 7 and 15); stakeholders can bring in their positions from an early stage on. Please note that ENTSO-E Stakeholder Committee does not have a rolling work programme as the Working Group will have, i.e. the Stakeholder Committee does not advises on deliverables.

***Question: When it comes to the Monitoring Body (Art. 16), do you think that the Network Code on Cybersecurity would benefit from ENTSO-E who is consulting instead of creating an entirely separate body such as Cybersecurity Working Group?***

Answer: The set-up of the Working Group and the Monitoring Body are different. The Monitoring Body advises ACER and is composed of institutional entities. Therefore, the Monitoring Body cannot replace the Working Group and vice-versa.

***Question: What happens in case of a violation of this Network Code? As far as we see, no penalties are foreseen.***

Answer: There is no specific penalty regime foreseen in the Network Code. Thus, national rules apply, i.e. national authorities (e.g. NRAs) can apply them at a national level. Penalties would be different in each Member State according to national legislation.

***Question: List of entities who are qualified as high and critical impact: will the transitional list be published but not the final list? Have you already considered potential risks that information, that is collected at an entity level and is centralized, could potentially be leaked? Does it add additional risk and how could we protect this from happening? The Network Code on Cybersecurity sets up a lot of principles on confidentiality, nevertheless, it is not sufficiently clear who has to do what. How the protection of information will be ensured?***

Answer: Indeed, information needs to be sufficiently protected and that is one, if not the main, building block (Title X of the Network Code). We need to find the right balance between transparency and data protection. We need a bottom-up flow of information (from entity level to the Member State to Union/regional risk management bodies) to adapt risk assessment methodologies and risk assessment practices to the evolving scenario of vulnerabilities and threats. At the same time this information flow must be confidential to protect the entity involved in the information exchange. There are three categories of data: EU level secret data, restricted information and unrestricted information. The Network Code on Cybersecurity explains what the sending and the receiving entity has to do. The objective is to avoid any harm / increased risks. However, some information will be needed for the cross-border risk assessment report (need to report to the European Commission and ACER). Regarding the transitional list – it will be made public because publication was explicitly included in the ACER Framework Guideline.

***Question: Does currently transparent data (e.g. on TP) be treated as protected data?***

Answer: Data that is already publicly available e.g. as on transparency platform will not be treated as protected / confidential data.

***Question: What is the definition of an entity at the level of the risk description? A physical installation or a company (legal notion)? What if the asset is operated by an entity having its headquarter in another country e.g. a wind turbine is operated by US company based in the US?***

Answer: In the Network Code on Cybersecurity there is a list of entities (Art. 2) to whom the Network Code applies. The entity is held responsible. For entities / service providers based in non-EU countries, specific provisions apply (Art. 2 para. 4).

***Question: Risk assessment (for potential electricity crisis) is already dealt with in Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 by NRAs and ACER - has this been considered and why is there a “new" risk management process the Network Code on Cybersecurity?***

Answer: Absolutely, the process and cycles for the risk assessment performed in the Regulation (EU) 2019/941 (Risk Preparedness Regulation) has been taken into consideration, as cyber risk is one of the risk scenarios considered in the National Risk Preparedness plans of most Member States. Nonetheless, a specialised cyber risk management approach, modeled after main international standards and frameworks, has to be adopted in order to take into account specific issues as the fast evolution of technologies and associated threats, the obligation already imposed by NIS Directive, the national approaches to cybersecurity (Cybersecurity national strategies) adopted by most member states. The Network Code on Cybersecurity is striving to combine the different risk assessments and exercises in order to avoid duplication.

***Question: Is the risk assessment at the entity level already harmonised with a basic set of standardised risks which can be supplemented by the entity? If each entity uses different risk description, the aggregation at Member State level can become quite complex.***

Answer: The point is perfectly valid and will be taken into account during the development of the methodologies (transitional period) of the Network Code on Cybersecurity.

***Question: The basic cybersecurity hygiene measures in Annex A lack e.g. a standardised risk management process and lack supply chain security controls. Isn`t this important for a common, minimum level of security? Many people are puzzled with Annex A. Security requirements are ultra-low and do not establish a sufficient level security in the entities. Micro and small business should have persons responsible for cybersecurity.***

Answer: Basic cybersecurity hygiene requirements have mainly to be applied by entities that have almost no impact on cross-border electricity flows, therefore, the requirements are kept very basic and minimal. The requirements stems from ENISA’s list of cybersecurity hygiene requirements, but we can consider listing higher requirements. Please provide proposals.

***Question: Shouldn't "verification guidance" be better provided by professionally accredited, conformity testing bodies?***

Answer: We put the responsibility on the entities to choose among different options to verify compliance, many parties could provide expertise for these purposes. Using a certified verification body is one of them (Art. 33).

***Question: Do you have a procedure for an occasion if a virus such as STUXNET is able to infect the whole electrical system? Did you describe also the process on how to recover from cyber incident/crisis or is this out of scope of this Network Code?***

Answer: This is included in this Network Code in the Article 40, 49 and whole Title VIII, where the crisis management is described and also the steps what to do when such an incident occurs. It foresees how countries coordinate to deal with such kind of cybersecurity electricity crisis. As a preemptive measure, diversification of vendors is one of the measures to ensure that one virus cannot affect the whole grid.

***Question: In the Supporting Document of the Network Code on Cybersecurity, IEC 62443 set of standards is mentioned, would they be the basis for harmonising procurement requirements for not only ICT products but also for developing the entity security management systems?***

Answer: There are many international standards that the Network Code is “inspired from”, but the choice of the standards that are to be applied in Europe, will be discussed by the Working Group e.g. when the procurement requirements are developed (Art. 15 and Art. 35).

***Question: Will the suppliers be categorised by their risk level?***

Answer: This will be decided during the implementation of the Network Code as the Network Codes only fixes the frame to develop specific criteria to identify high impact and critical impact entities and the respective requirements / controls that are to be applied.

***Question: If a daughter companies) is an electricity undertaking (generation, supply), does this implies that the mother company and other daughter companies fall under the scope of the Network Code?***

Answer: It depends on what is the activity of the mother company and the daughter companies, i.e. whether they are also electricity companies and whether they are under the scope of the NCCS (Art. 2).

***Question: How the Standards mapping matrix would work and what key references would be considered?***

Answer: The Standard mapping matrix (Art. 25) will collect relevant International standards and national legal requirements and map them to Network Code on Cybersecurity controls.

***Question: Can you link the advanced cybersecurity controls to the level of RESTREINT-EU? All Member States are familiar with that.***

Answer: This level will most probably be included in the Standards mapping matrix where all relevant international, European and national legislations/standards will be mapped (Art. 25).