

A NEW ASSOCIATION FOR THE EUROPEAN DISTRIBUTION SYSTEM OPERATORS (DSOS) The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."



NETWORK CODE ON CYBERSECURITY

PUBLIC CONSULTATION WORKSHOP 19TH NOVEMBER 2021 WE START AT 14:03

ORGANISATION DETAILS



Workshop planning: 3 hours

Ih10 presentations & Ih50 Q&A session



All participants are muted



All the questions and comments received in the MT chat will be considered after the workshop



During the Q&A the participants can raise the hand to ask a question / make a comment



INTRODUCTION & RECAP

ANDREA FOSCHINI

A NEW ASSOCIATION FOR THE EUROPEAN DISTRIBUTION SYSTEM OPERATORS (DSOS) The EU DSO Entity



WHY A NETWORK CODE ON CYBERSECURITY FOR THE ELECTRICITY SECTOR

The global scenario of cyber threats is getting worse...

Electricity sector is not standard...



News of January 2017...



Energy transition and associated digitalization is enlarging the cyber-attack surface...



NETWORK CODE FOR <u>CYBERSECURITY ASPECTS OF CROSS</u> BORDER ELECTRICITY FLOWS

The development of the network codes follows the rules of Regulation (EU)2019/943

• network code contains <u>legally binding</u> rules / every entity within the scope of the network code will have to comply.

 while the network code will not duplicate national regulation, <u>national regulation</u> <u>have to be consistent and may have to adapt to the network code</u>. Hence, creating <u>fit-for-purpose</u> network codes is in everyone's interest.

• <u>Stakeholder</u> engagement is crucial.

THE TIMELINE (BIRD'S VIEW)

THE TIMELINE... WHERE WE ARE NOW?

PROJECT	ТАЅК	START	PLAN END	
Phase 1 NC CS v1	Drafting NC CS Version 1 (DT) Drafting Committee review Transpose the NC CS v1 in legal text Deliver the revised NC CS v1 (DT)	27/07/2021	11/11/2021	\checkmark
Phase 2 NC CS public consultation	Stakeholders' updates NC CS public consultation Public Consultation Workshop 1 Public Consultation Workshop 2 (December 08th, 2021)	12/11/2021	10/12/2021	
Phase 3 NC CS v2	Incorporate all comments from public consultation (DT) Deliver NC CS v2 (DT0 Drafting Committee' review Submit NC CS final to ACER	13/12/2021	14/01/2022	_

LEGAL FRAMEWORK & GENERAL PROVISIONS

SABINE HINZ

PARTICULARITIES OF THIS NETWORK CODE

- The Cyber Security Network Code is not the 1st Network Code <u>BUT</u> it is the 1st Network Code
 - to be (co)drafted by DSOs and TSOs
 - to be drafted according to the new Clean Energy Package rules
 - to be drafted in less than 6 months (!)
 - that will cover also responsibilities of very diverse bodies
 - at EU level (e.g. ACER, ENISA, ENTSO-E, EU DSO entity, NEMOs)
 - at regional level (e.g. RCC)
 - national level (e.g. NRAs, RP-NCAs, CS-NCAs, CSIRTs)
 - that is to be drafted when some of the main legislation on cyber security is under revision (e.g. NIS 2.0 Directive)
- \rightarrow Many challenges to be tackled at once in the network code development phase.

TITLE I GENERAL PROVISIONS

I. Scope (Article 2)

- a. defining to whom the NCCS will apply;
- b. territorial scope (e.g. relations with 3rd country parties).

2. Definitions (Article 4)

- a. alignment throughout all chapters;
- b. adding new definitions that are necessary;
- c. consistency check with ACER framework guideline.

3. Approval, amendment and consultation procedures (Articles 5-8)

- a. methodology-approach as in other Network Codes
- b. broad stakeholder involvement
- c. regulatory oversight

4. Monitoring and benchmarking (Articles 12 and 13)

- a. standard clauses
- b. BUT more actors involved, such as ENISA, RCCs, CS-NCA

Questions for the public consultation

- Are the objectives (Article 3) of the network code clear?
- Is the timing in the network code to implement the provisions and develop the deliverables feasible (e.g. Article 2, Article 14, Article 49, Article 50)?
- Do you think these requirements for small and micro enterprises are of sufficient level (Article 2 + Annexe I)?
- Do you agree with the monitoring and benchmarking approach (Articles 12 +13)?

NCCS – STRUCTURE OF WORK

CHRISTIANE GABBE

A NEW ASSOCIATION FOR THE EUROPEAN DISTRIBUTION SYSTEM OPERATORS (DSOS) The EU DSO Entity

NETWORK CODE CYBERSECURITY (NCCS) ORGANIZATIONAL STRUCTURE FOR DRAFTING

Drafting Committee	Article 59(3) or (10) of Regulation (EU) 2019/943: a Drafting Committee shall be convened
	It shall consist of representatives of ACER, ENTSO-E, EU DSO Entity, and where appropriate NEMOs*) and a limited number of the main affected stakeholders.
	Objective: guaranteeing early involvement of relevant stakeholders in the drafting process
	Co-chaired by ENTSO-E and EU DSO Entity
	→ Act like a 'advisory committee'

De	velopment Team
	Sub

- The Development Team shall prepare proposals for the scope, proposals on content with different options if relevant and a first text of the network code or guideline
- Staffed by experts from ENTSO-E and EU DSO Entity
- Review and amend draft text upon public consultation
- Various subgroups preparing text
- → Performing actual drafting

(*) Nominated Electricity Market Operators

NETWORK CODE CYBERSECURITY (NCCS) SCOPE & SUMMARY OF NCCS CONTENT

General Chapter (Framing)

a. common understanding of terminology (what are we talking about).
 c. clear delimitation of scope (who has to apply the provisions)

b. protection of sensitive data (what can be shared with whom and in which format)
 d. check of implementation and efficiency of the NCCS provisions (is the NCCS efficient)

Cross-Border Risk Management	Certification/Verification	Sharing of Technical Information	Product Certification
 Goals: Overall current cyber-risk picture of the European energy grid Identification of (unacceptable) cyber risks generate a cyber-risk treatment plan risk treatment by mandatory & optional security controls 	 Goals: Set-up Risk Management at individual electricity entity level Create a Common Electricity Cybersecurity Framework Create mandatory cybersecurity hygiene requirements for all entities Create minimum and advanced cybersecurity requirements for high risk and critical risk entities Setup Verification Process of requirement implementation for critical risk entities 	 Goals: Information collection, sanitization and dissemination and handling of incident information Cybersecurity Early Warning System for the energy sector Built an Electricity Cybersecurity Exercise Framework Set-up Crisis Management procedures Assure protection of information exchanged in that context 	 Goals: Sets Controls on the procurement processes of high-risk and critical-risk entities to ensure they procure secure equipment Harmonize security requirements and verification methods to support entities in implementing the controls

INTRODUCTION TO THE TECHNICAL CHAPTERS

MAARTEN HOEVE

A NEW ASSOCIATION FOR THE EUROPEAN DISTRIBUTION SYSTEM OPERATORS (DSOS) The EU DSO Entity

RISK BASED APPROACH

ENTITIES IN SCOPE DETERMINED BY IMPACT

SCOPE WITHIN AN ENTITY DETERMINED BY IMPACT

RISK ASSESSMENT PERFORMED EVERY TWO YEARS

Union-wide impact assessment report (year 1)	Cross-border electricity cybersecurity report (year 2)
 Information to determine scope: High-/critical-impact processes with impact ECII and high-/critical-risk thresholds Harmonized risk matrix 	 Information to determine controls: Aggregated risks Regional risk treatment plan Common electricity cybersecurity framework Minimum and advanced cybersecurity controls Controls to standards mapping matrix

TRANSITIONAL PERIOD TO LET ENTITIES PREPARE

NETWORK CODE CYBERSECURITY – THE GRID OPERATORS VIEW

PETER PONGRACZ & OLIVIER CLEMENT

Reliable Sustainable Connected

A NEW ASSOCIATION FOR THE EUROPEAN DISTRIBUTION SYSTEM OPERATORS (DSOS) The EU DSO Entity

TITLE VIII : INCIDENT & CRISIS MANAGEMENT, INFORMATION SHARING

TITLE IX : CYBERSECURITY EXCERCISES

CROSS BORDER CYBER RISK MANAGEMENT & FUNCTIONAL SECURITY REQUIREMENTS

KEITH BUZZARD & BART LUIJKX

Reliable Sustainable Connected

A NEW ASSOCIATION FOR THE EUROPEAN DISTRIBUTION SYSTEM OPERATORS (DSOS) The EU DSO Entity

FOCUS AREAS OF NETWORK CODE ON CYBERSECURITY

COMMITMENTS FOR ENTSO-E AND EU DSO ENTITY I

ENTSO-E and EU DSO entity are responsible and perform with the stakeholders the following tasks:

- identify Critical Business Processes which could pose critical operational and safety issues to the resilience of cross border electricity flows; maintain a Risk Impact Matrix (RIM) together with appropriate operational limit thresholds for the purposes of cross-border electricity flow cyber risk evaluation purposes; perform a top-down risk assessment on every Critical Business Process identified, using internationally recognized techniques such as Business Impact Analysis (BIA) together with the Smart Grid Architecture Methodology (SGAM) model to perform threat modelling and derive appropriate security controls.

- introduce an **integrated top-down and bottom-up cybersecurity risk assessment methodology**, together with an **Electricity Cybersecurity Risk Index** (ECRI), including:

ECRI Caps (thresholds) for defining critical-risk and high-risk entities

An index to determine when small and micro enterprises shall be classified as high risk or critical-risk entities Basic cyber hygiene requirements to be implemented by small and micro enterprises who are not critical-risk or highrisk entities.

COMMITMENTS FOR ENTSO-E AND EU DSO ENTITY II

- determine the specific <u>cybersecurity risks exposures of the different entities to cross-border</u> <u>electricity flows</u>, which allows the CS-NCAs and the NRAs to classify all these entities in their territory into a transitional list of "critical-risk" / "high-risk" entities.

- prepare a transitional list of **prominent International standards and national legislation on electricity cybersecurity** to be implemented by entities in preparation for the implementation of the common electricity cybersecurity framework.

- maintain a **<u>Regional cyber risk treatment plan</u>**, which shall be complementary to the Cross-Border Electricity Cybersecurity Risk Assessment Report.

- a description of mandatory and/or advisory—only functional security controls providing adequate protection (assurance) against cyber-attacks;

- a description of advisory-only, non-functional security requirements, such as quality, assurance level and compliance to national or international standards.

- the results of the integrated top-down and bottom-up cybersecurity risk assessment shall be consolidated in a **Cross-Border Electricity Cybersecurity Risk Assessment Report**, which shall assess and certify the improved state of the cybersecurity posture of the electricity sector and shall include Critical Business Processes which shall act as the reference for compliance and product assurance activities.

COMMITMENTS FOR ENTSO-E AND EU DSO ENTITY III

- provide an **Electricity Requirements and Standards Mapping Matrix (ERSMM)**. The ERSMM shall map requirements of the common electricity cybersecurity framework to requirements of selected legislative frameworks and internationally recognized standards.

- monitor the effectiveness of ECEWS (European Cybersecurity Early Warning System). * delegated to ENISA *

- organize a multi-year program of electricity cybersecurity exercises, shall organize a mandatory regional cybersecurity exercise every 3 years, shall perform periodic analysis of lessons learned and recommendations for follow-up activities, prepare on a yearly basis an exercise template based on major risks, shall develop a voluntary cybersecurity simulation testbed.

-develop a sector-specific guideline on EU products/services/systems verification schemes.

CERTIFICATION

CHRISTIANE GABBE

A NEW ASSOCIATION FOR THE EUROPEAN DISTRIBUTION SYSTEM OPERATORS (DSOS) The EU DSO Entity

DEVELOPMENT OF CERTIFICATION TOPIC

Original idea - according to the Final report of the informal drafting team: Achieving a baseline level of cybersecurity by common ISO/IEC 27001 certification (or equivalent)

CERTIFICATION

A NEW ASSOCIATION FOR THE EUROPEAN DISTRIBUTION SYSTEM OPERATORS (DSOS) The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."

SUPPLY CHAIN SECURITY AND PRODUCT ASSURANCE

MAARTEN HOEVE

INTEGRATED APPROACH TO SUPPLY CHAIN SECURITY

HARMONIZED REQUIREMENTS AND VERIFICATION

DISCUSSION SESSION

A NEW ASSOCIATION FOR THE EUROPEAN DISTRIBUTION SYSTEM OPERATORS (DSOS) The EU DSO Entity

NEW ASSOCIATION FOR THE EUROPEAI TRIBUTION SYSTEM OPERATORS (DSO

nts of this been formally established by the Electricity

943 "in order to increase efficiencies in the electricity d in the Union and to ensure close cooperation with trans system operators and the ENTSO for Electricity."

NETWORK CODE ON CYBERSECURITY

ole Sustainable Connecte

WORKSHOP: PUBLIC CONSULTATION, 19 NOVEMBER 2021

A NEW ASSOCIATION FOR THE EUROPEAN DISTRIBUTION SYSTEM OPERATORS (DSOS) The EU DSO Entity

The EU DSO Entity has been formally established by the Electricity Regulation (EU) 2019/943 "in order to increase efficiencies in the electricity distribution networks in the Union and to ensure close cooperation with transmission system operators and the ENTSO for Electricity."

BACK-UP

TITLE I – GENERAL PROVISIONS / ARTICLE 2 SCOPE

#	Table I. Entity definition
I	Electricity undertakings as defined in Article 2(57) of the Directive (EU) 2019/944
2	NEMOs as defined in Article 2(7) and (8) of Regulation (EU) 2019/943
3	Electricity digital market platforms as defined in the ACER Framework Guideline
4	Critical service providers as defined in the ACER Framework Guideline
5	Regional Coordination Centres (RCCs) established pursuant to Article 35 of the Regulation (EU) 2019/943
6	ENTSO-E, the EU DSO entity, ACER and NRAs as defined in Regulation (EU) 2019/943 and Directive (EU) 2019/944
7	RP-NCAs, SOCs, CS-NCAs and CSIRTs and ENISA as defined in Regulation (EU) 2019/941, in Directive (EU) 2016/1148 and Regulation (EU) 2019/881

From the principles in the ACER Framework Guideline...

SUPPLIERS ENTSO-E EU D CSIRT Service Entity **Providers** RCC ACER EUROPEAN COMMISSION **CS-NCA NRA NEMOs** ENISA **RP-NCA**

... to the legal text of the network code.