Cybersecurity in the energy sector

E.DSO/ESMIG Webinar ‘Is EU regulation supporting the cyber revolution for the energy sector?’, 16 May 2023

Michaela Kollau

DG ENERGY, Unit B4: Energy security and safety

Cybersecurity in energy: context

- **The electricity sector in the Union is undergoing a profound transformation**, characterised by more decentralised markets with more players, a higher proportion of energy from renewable sources, and more digitalised and interconnected systems
- The **digitalisation of the energy system** can deliver a strong contribution to energy security and climate goals, by making our energy system more efficient, more flexible and more resilient.
- But it **also brings along new challenges** related to the cybersecurity of our European energy infrastructure and the reliance of its electricity grid.
- **Cybersecurity** is, now more than ever, a **key horizontal requirement for a secure and robust energy system.**

European Commission cybersecurity policy landscape

- Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2) – 2022
- Proposal for a Regulation on cybersecurity requirements for products with digital elements, known as the Cyber Resilience Act (CRA) - 2023
- Directive on the resilience of critical entities (CER) – 2022
- The Digital Operational Resilience Act (DORA) - 2022
- Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure – 2022
- Radio Equipment Directive Delegated Act on cybersecurity
- EU Cybersecurity Act - 2019
- Commission Recommendation on cybersecurity in the energy sector & and Staff Working Document - 2019
- Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (NCCS) - planned for 2023

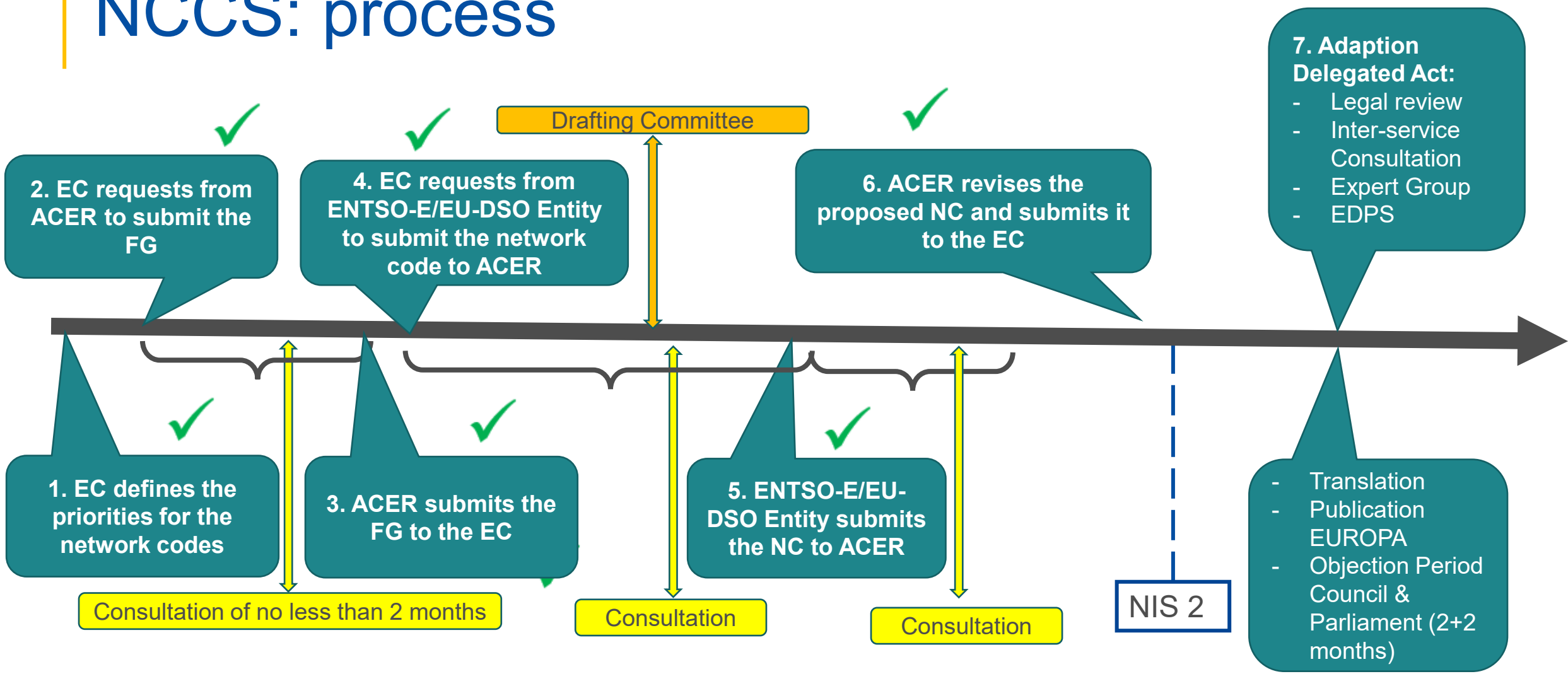
Network Code on cybersecurity: legal basis

- **Electricity Regulation (EU) 2019/943, Article 59 (2)** empowers the Commission to adopt a delegated acts supplementing this Regulation in accordance with Article 68 concerning the establishment of network codes in respective areas.
- For cybersecurity the **Article 59 (2) (e) foresees sector-specific rules for cyber security aspects of cross-border electricity flows, on common minimum requirements, planning, monitoring, reporting and crisis management.**

Why a NCCS?

- Specific characteristics of the energy sector
- Cybersecurity legislation  Electricity legislation
- Cyber “world”  “Energy world”
- Specific Solution

NCCS: process



European Commission

NCCS: State of play

- ACER has reviewed the proposed network submitted by ENTSO-E and EU DSO Entity to ensure it complies with the relevant Framework Guidelines and contributes to market integration, non-discrimination, effective competition and the efficient functioning of the market.
- Commission (DG ENER) has received it and has started the adoption process. Currently the legal team from DG ENER and the Legal Service of the Commission and DG CNECT are reviewing the text.
- Next step: consultation of expert group
- Presented in WS energy NIS Cooperation Group on 17.3.22, 21.09.2022 and Council Horizontal Working Party on Cyber on 8.12.2021, 22.3.2022 & bilateral discussions with MS authorities and associations

NCCS: Scope and objectives

- Applies to a subsector of the Energy sector, **Electricity**. Within electricity subsector, the scope of applicability is limited to entities with impact on **cross-border** electricity flows. The **risk assessment** will identify which entities are most relevant and what **security measures** they need to apply.
- **Complementing and building upon NIS2** to include sector-specific cybersecurity requirements.
- It provides more **precise instructions and procedures**, designed by electricity **stakeholders** together with cybersecurity **experts**, for the **electricity sector.**
- The NCCS specifies measures in a **coordinated way** with industry contribution and the outcome is ready to be used by different **Competent Authorities**.

The NCCS will contribute to the security of supply in cross-border flows of electricity by…

- Providing for a continuous and comprehensive approach to carry out all steps from the risk assessment to the risk treatment and continuous improvement.
- Providing clear roles and instructions to carry out such steps by different stakeholders and authorities, electricity and cyber, including their interactions (what, when, how).
- Contributing to a higher common level of cybersecurity across the Union, providing guidance on how to identify and implement specific controls
- Enhancing information sharing (timely and fast) between electricity undertakings and cybersecurity bodies in EU on cyber vulnerabilities and incidents.
- Defining and coordinating the electricity and cybersecurity procedures when handling electricity incidents and crises with a cyber component;
- Defining procedures for an exercise framework to enhance preparedness of all operators to deal with electricity incidents with cybersecurity components;
- Providing a set of rules for the protection of information exchange among the different stakeholders in electricity and cyber domains;
- Providing for a framework for monitoring, benchmarking and reporting

Thank you

European Commission