Energy Community

THE ENERGY COMMUNITY

The Clean Energy Package and Cybersecurity

5th CyberCG Meeting

16 December 2021, Session II – Cybersecurity Legislation in the Energy Community

MAIN AREAS OF WORK

- Statistics
- Electricity
- Renewable energy
- Value added tax
- Competition/ state aid
- Environment
- Cyber security
- Regulator
- Gas
- Climate
- Energy efficiency
- Oil
- Security of energy supply
- General services

Clean Energy Package as adopted in EnC

- provisions relevant for cybersecurity in the ELECTRICITY sector

- Governance Regulation - REGULATION (EU) 2018/1999 of 11 December 2018 on the Governance of the Energy Union and Climate Action, amending Regulations (EC) No 663/2009 and (EC) No 715/2009, Directives 94/22/EC, 98/70/EC, 2009/31/EC, 2009/73/EC, 2010/31/EU, 2012/27/EU and 2013/30/EU Directives 2009/119/EC and (EU) 2015/652 and repealing Regulation (EU) No 525/2013

- Electricity Directive - DIRECTIVE (EU) 2019/944 of 5 June 2019 on common rules for the internal market for electricity

- Risk Preparedness Regulation - REGULATION (EU) 2019/941 of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC

EnC - Clean Energy Package and cybersecurity

❑ Governance Regulation

- Five dimensions - (a) energy security; (b) internal energy market; (c) energy efficiency; (d) decarbonisation; (e) research, innovation and competitiveness
  - National objective - addressing constrained or interrupted supply of an energy source, for the purpose of improving the resilience of regional and national energy systems, including a timeframe when the objectives should be met;
  - Integrated reporting - on the ability to cope with constrained or interrupted supply of an energy source, including gas and electricity:
    - implemented, adopted and planned policies and measures
    - regional cooperation in implementing the objectives and policies
    - financing measures in this area at national level
  - Potential negative impacts on the security of supply and grid stability in small or isolated energy systems from renewable energy contributions
  - Bioenergy sustainability - security of supply implications from biofuels, bio-liquids and biomass [including transport and treatment of HYDROGEN, METHANE and GHG]

EnC - Clean Energy Package and cybersecurity

❑ Electricity Directive

- Security of supply – indirect references
- Authorization procedure – criteria for granting authorization for the construction of generation capacity considering the safety and security of the electricity system, instalations and associated equipment
- Data protection – organized in order to ensure efficient and secure data access and exchange, as well as data protection and data security
  - Task of the TSO – data management, including the development of data management systems, cybersecurity and data protection, subject to the applicable rules, and without prejudice to the competence of other authorities
  - IT systems – ITO shall not share IT systems or equipment, physical premises and security access systems with any part of the vertically integrated undertaking nor use the same consultants or external contractors for IT systems or equipment, and security access systems.
- Smart metering – smart metering systems
  - Functionality – compliance with relevant applicable security rules, having due regard for the best available techniques for ensuring the highest level of cybersecurity protection while bearing in mind the costs and principles of proportionality
  - Deployment - taking into consideration best available techniques for ensuring the highest level of Cybersecurity and data protection

EnC - Clean Energy Package and cybersecurity

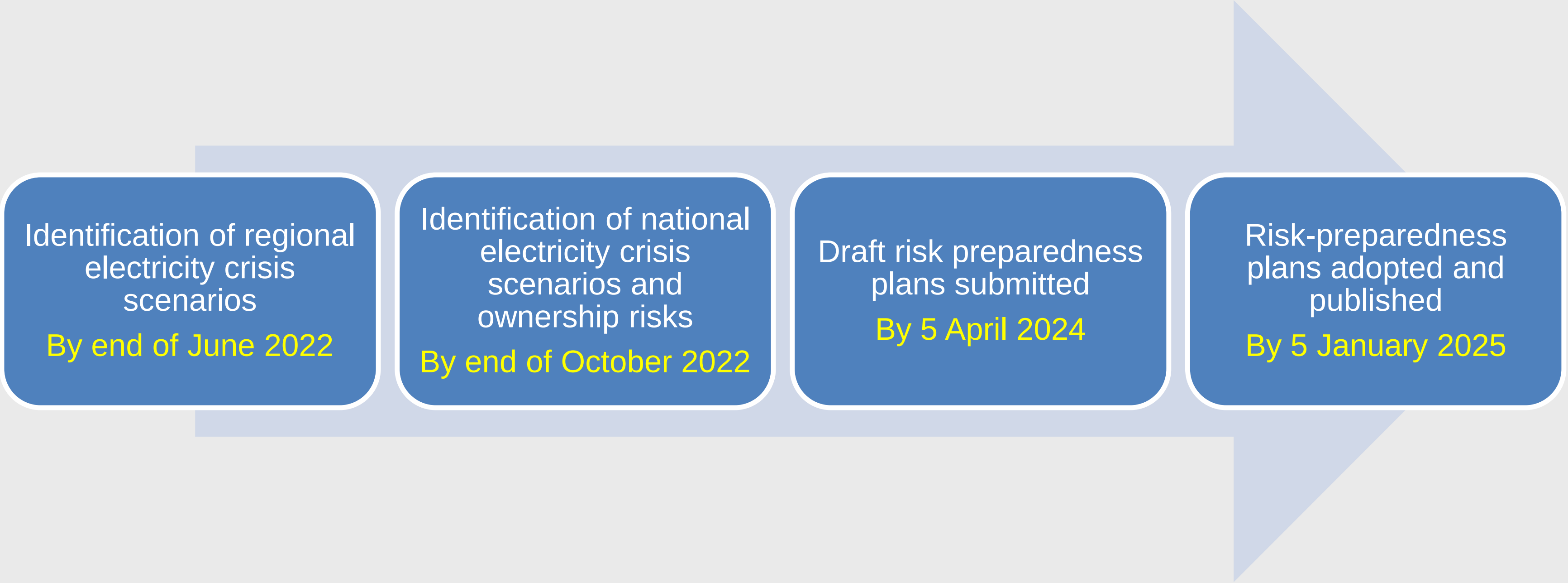
❑ Risk Preparedness Regulation

- Security of electricity supply – rules for cooperation between CPs with a view to prevent, prepare for, manage, evaluate and monitor electricity crises
- SoS Coordinatuion Group – established by PA 2008/02/MC-EnC, PA 2021/03/MC-EnC - given a major role
- Competent authority – to be appointed (national government or regulatory authority / delegated tasks)
- Risk managemnet
  - Risk assessment - cybersecurity risks included
    - Methodology – same as defined and applied in the EU
    - Regional electricity crisis scenarios (regions identified as synchronous areas)
    - Most relevant national electricity crisis scenarios / ownership risks
  - Adequacy assessment (short-term / seasonal) – same EU Methodology
  - Risk Preparedness Plans – consists of national, regional and, where applicable, bilateral measures
    - Consistency of (national) risk preparedness plans and their publication
    - Content of risk preparedness plans – national / regional / bilateral measures
    - Assessment of risk preparedness plans

EnC - Clean Energy Package and cybersecurity

❑ Risk Preparedness Regulation

- Risk Management IMPLEMENTATION timeline



Identification of regional electricity crisis scenarios
By end of June 2022

Identification of national electricity crisis scenarios and ownership risks
By end of October 2022

Draft risk preparedness plans submitted
By 5 April 2024

Risk-preparedness plans adopted and published
By 5 January 2025

EnC - Clean Energy Package and cybersecurity

❑ Risk Preparedness Regulation

- Electricity Crisis managemnet
  - Early warning – declaration of electricity crisis
    - the measures set out in the risk-preparedness plan shall be followed to the fullest extent possible
  - Cooperation and assistance among the Contracting Parties
    - regional or bilateral measures that have been agreed
    - technical, legal and financial arrangements
    - fair compensation criteria
    - compliance with market rules
  - Ex-post evaluation and reporting
- Monitoring by the SoS Coordination Group
- Confidentiality criteria

EC Recommendations on Cybersecurity in energy

EC Recommendation C(2019)2400, and corresponding Staff Working Paper SWD(2019)1240 :

❑ **Real-time requirements** - some energy systems need to react so fast that standard security measures such as authentication of a command or verification of a digital signature can simply not be introduced due to the delay these measures impose.

❑ **Cascading effects** - electricity grids and gas pipelines are strongly interconnected across Europe and well beyond the EU. An outage in one country might trigger blackouts or shortages of supply in other areas and countries.

❑ **Combined legacy systems with new technologies** - many elements of the energy system were designed and built well before cybersecurity considerations came into play. This legacy now needs to interact with the most recent state-of-the-art equipment for automation and control, such as smart meters or connected appliances, and devices from the Internet of Things without being exposed to cyber-threats.

EC Recommendations on Cybersecurity in energy

Real-time Requirements

- Use international standards
- Apply physical measures
- Classify / manage your assets
- Consider privately owned communication networks, or consider specific measures
- Consider splitting systems into logical zones
- Choose secure communication and authentication

Cascading effects

- Evaluate interdependencies
- Ensure communication framework for early warnings and to cooperate in crisis
- Ensure level of security for new devices
- Consider cyber - physical spill overs
- Establish design criteria for a resilient grid

Technology mix

- Follow a cybersecurity-oriented approach when connecting devices
- Use international standards
- Establish monitoring and analysis capabilities
- Conduct specific cybersecurity risk analysis for legacy installations
- Collaborate with technology providers
- Update hardware and software

MC-EnC Cybersecurity Procedural Act (29 November 2018)

- Domains (of critical infrastructure / essential services in):
  - Electricity / Natural gas / Oil / pollution and combustion emissions
  - Digital and electronic communications (services provided to energy operators)
- Stakeholders
  - Ministries (energy / climate / digital communications & information technologies),
  - NRAs
  - Operators of critical infrastructure / essential services (Production / TSOs / DSOs)
  - National Cybersecurity Competent Authorities / CSIRTs

MC-EnC Cybersecurity Procedural Act (29 November 2018)

- Applied EU *acquis* provisions from:
  - on Electronic communications networks and services – Directive 2002/21/EC
  - on Critical Infrastructures Directive (identification / designation / protection) – Directive 2008/114/EC
  - on Security of network and information systems - NIS Directive – Directive (EU) 2016/1148
  - European standardization in information security - Regulation No. 1025/2012/EU

MC-EnC Cybersecurity Procedural Act (29 November 2018)

- Tasks
  - establish administrative and operational environment (focal points / liaison officers)
  - communicate information (reports / strategies / measures) and knowledge (training / research and development / public awareness)
  - Develop and apply EU-coherent methodologies for risk assessment / security criteria / identification and designation of essential services and critical infrastructures,
  - apply EU technical standards on information security and relevant technologies,
  - establish a CSIRTs network (security incidents and threats / capacity building / blueprint for cooperation and early warning / mutual assistance)
  - facilitate cooperation with EU MSs / gaining observers’ status in ENISA

THANK YOU for your attention

simon.uzunov@energy.community.org

www.energy-community.org

Ener_Community

/company/energy-community

/Ener.Community

/EnergyCommunityTV

EnC CyberCG Work Plan 2022

❑ ECS – Cybersecurity Highlights in 2021

- Comments provided to NIS 2 Directive (CP Support to the WEF Recommendations)
- Proposed Amendments for NIS 2 (ECS)
- Comments on the ACER Framework Guidelines (ECS)
- Comments on the ENTSO-E Cybersecurity NC (ECS)
- EnC Annual Implementation Report 2021 (ECS)
- Main EVENTS:
  - WS with WEF on the NIS 2 Directive – April 2021
  - Energy Community Cyber Day – June 2021
  - CyberCG Annuel Meeting – December 2021

❑ CyberCG – Activities in 2022

- Steps in Implementation of the CEP (in cooperation with SoS CG)
  - Adoption of a Roadmap and Policy Guidelines - CyberCG
  - Establishment of Cybersecurity Risk Assesment Framework (Rules, Methodology, Reporting mechanism)
  - Adoption of Cybersecurity Risk Preparednes Plan (template)
  - Development of Cybersecurity Crisis Managemnet Mechanism
- Cybersecurity Network Code, NIS 2 Directive (energy)
  - Early implementation mechanisms
- Eenrgy Community ISAC - Initiative for establishment
- Implementation Report 2022
- EVENTS (tentative)
  - WS on the implementation of Cybersecurity NC and NIS 2 Directive in EnC (2)
  - WS with WEF on Cyber resilience (training for NRA)
  - WS on the establishment of EnC ISAC
  - Cyber Day
  - CyberCG Meetings (2)