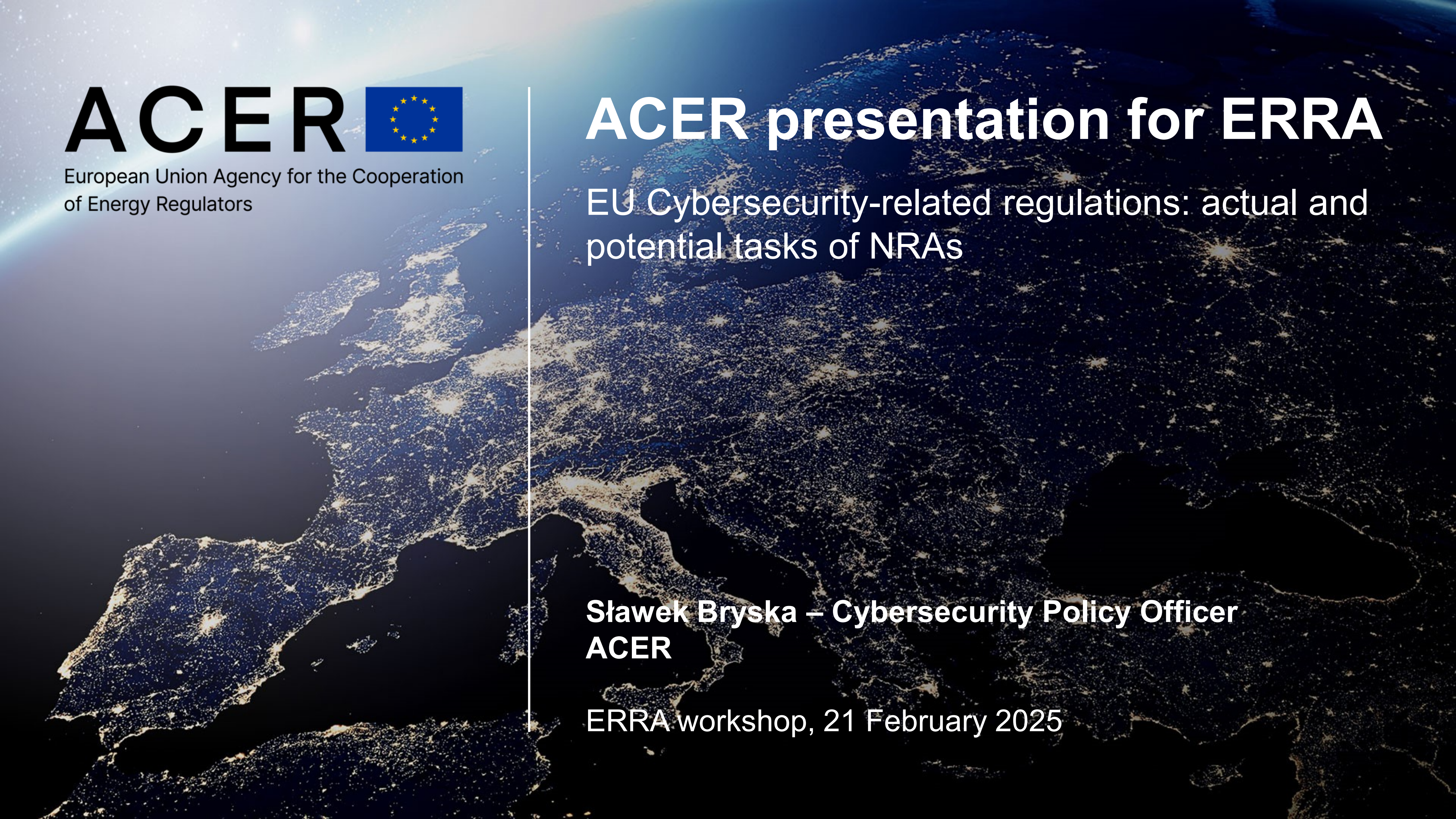


ACER

European Union Agency for the Cooperation of Energy Regulators

ACER presentation for ERRA

EU Cybersecurity-related regulations: actual and potential tasks of NRAs

Sławek Bryska – Cybersecurity Policy Officer
ACER

ERRA workshop, 21 February 2025

Scope of the presentation

‘Actual and potential’ tasks	Legislation either gives the task to the NRA explicitly or the NRA could be designated as an authority with specific tasks under that legislation.
‘Cybersecurity-related’	Cybersecurity Network Code for Electricity Risk Preparedness Regulation for Electricity

Cybersecurity Network Code for Electricity (NCCS)

NCCS entered into force on 13 June 2024

NCCS is primarily a tool for developing more detailed rules

It provides a governance model and objectives for the development of terms and conditions, methodologies and plans.

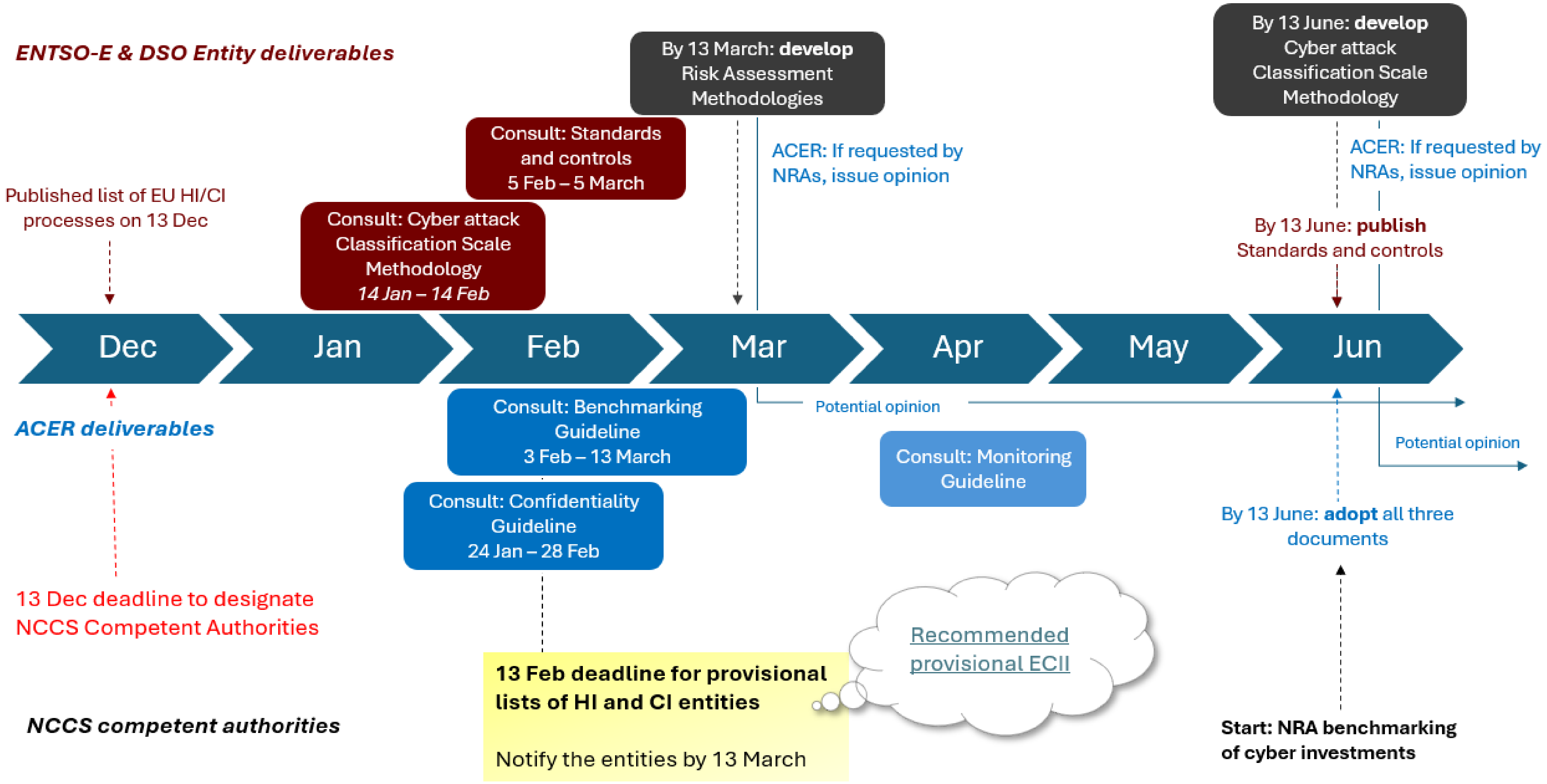
Each Member State shall designate a competent authority to carry out the tasks assigned to it under the NCCS…

Designation by 13 December 2024. Until the competent authority has been designated, the NRA shall carry out its tasks

…including supervising 'high-impact' and 'critical impact' entities

Such as TSOs, DSOs, suppliers, generators, aggregators, NEMOs, organised markets, balancing responsible parties, operators of recharging points and critical ICT service providers.

Indicative timeline of H1 2025



ENTSO-E & DSO Entity deliverables

Published list of EU HI/CI processes on 13 Dec

Consult: Cyber attack Classification Scale Methodology *14 Jan – 14 Feb*

Consult: Standards and controls 5 Feb – 5 March

By 13 March: **develop** Risk Assessment Methodologies

ACER: If requested by NRAs, issue opinion

By 13 June: **develop** Cyber attack Classification Scale Methodology

ACER: If requested by NRAs, issue opinion

By 13 June: **publish** Standards and controls

ACER deliverables

Consult: Benchmarking Guideline 3 Feb – 13 March

Consult: Confidentiality Guideline 24 Jan – 28 Feb

Potential opinion

Consult: Monitoring Guideline

Potential opinion

By 13 June: **adopt** all three documents

13 Dec deadline to designate NCCS Competent Authorities

NCCS competent authorities

13 Feb deadline for provisional lists of HI and CI entities

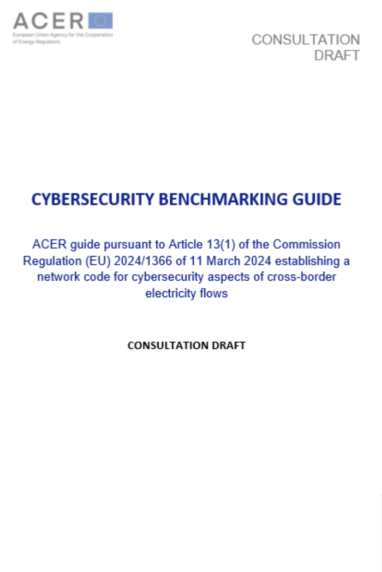
Notify the entities by 13 March

Recommended provisional ECII

Start: NRA benchmarking of cyber investments

Tasks of NRAs under the NCCS

Benchmarking cybersecurity investments

NRA task pursuant to the NCCS	ACER supporting deliverable	ACER Cybersecurity Task Force
Assess efficiency of cybersecurity investments, including: • Risk mitigation • Procurement integration • Average company expenditure • Average prices of cybersecurity services and products • Existence of comparability of their costs and functions • How cost-efficiency could be improved	Benchmarking guideline  CONSULTATION DRAFT **CYBERSECURITY BENCHMARKING GUIDE** ACER guide pursuant to Article 13(1) of the Commission Regulation (EU) 2024/1366 of 11 March 2024 establishing a network code for cybersecurity aspects of cross-border electricity flows CONSULTATION DRAFT	Collaboration on the benchmarking guideline Collaboration on the benchmarking exercise

NCCS compliance cost assessment

NRA task pursuant to the NCCS	ACER Cybersecurity Task Force
Assess whether the NCCS compliance costs borne by the TSOs and the DSOs are reasonable, efficient and proportionate If so, the TSOs and the DSOs will be able to recover them via network tariffs	Exchange best practices

Union-level crisis management plan for electricity sector

NRA task pursuant to the NCCS	ACER Cybersecurity Task Force
Closely cooperate with ACER to develop a Union-level cybersecurity crisis management plan	Forum for cooperation with the NRAs in the development of the crisis management plan Other stakeholders involved: ENISA, ENTSO-E, EU DSO entity, cybersecurity competent authorities, NCCS competent authorities, risk preparedness authorities and the national cyber crisis management authorities

European Cybersecurity Stakeholder Committee *(planned)*

	NCCS Article	Task
Different scope from other committees	10	Identifying problems and proposing improvements related to the implementation of the NCCS
	12(2)(b)	Identifying whether additional rules on common requirements, planning, monitoring, reporting and crisis management may be necessary to prevent risks for the electricity sector
	12(2)(c)	Identifying areas of improvement for the revision of the NCCS or determining uncovered areas and new priorities that may emerge due to technological developments
Wide landscape of public and private sector stakeholders		Once established, it would include NRA representatives

Main tasks of NRAs if designated as NCCS Competent Authorities

‘The minimum’

Article 5	Cooperation between relevant authorities and bodies at national level
Article 4(3), first sentence	Member States may allow their competent authority to delegate any NCCS task except for the tasks listed in Article 5

Decisions on terms, conditions, methodologies and plans

To be approved by all Competent Authorities in...	TCMP
...the EU	Cybersecurity risk assessment methodologies (TSOs' proposal by 13 March 2025)
	Cyber-attacks classification scale methodology (TSOs' proposal by 13 June 2025)
	Minimum and advanced cybersecurity controls, including for the supply chain
	Mapping of cybersecurity controls against standards
	Comprehensive cross-border electricity cybersecurity risk assessment report
...each relevant SOR	Regional cybersecurity risk mitigation plans

Analysis of risk assessments submitted by the entities

Designation of high-impact and critical-impact entities	Using the Electricity Cybersecurity Impact Index. May also entity groups of entities
Entities shall report to the Competent Authorities:	Controls selected to address risks with their implementation status Risk estimate for each Union-wide HI/CI process* and relevant assets ICT service providers for the CI processes

*Could be, for example, TS or DS monitoring and control, protection against faults, operational security analysis, outage planning and coordination, schedule management, TS defence or restoration

Supervision of entities – supply chain security (1)

Entities will need to...

...take into account procurement recommendations on, for example:	Secure and controlled design, development and production of ICT products, services and processes, including their technical security
	Support for security updates throughout the entire lifetime of these products
	Traceability of the application of security specifications from development to delivery
...and select suppliers that meet cybersecurity specifications	These criteria will be developed under the NCCS as part of ICT procurement recommendations

Supervision of entities – supply chain security (2)

Cyber Resilience Act (Oct 2024)

Cybersecurity requirements for products, including:	No known exploitable vulnerabilities, access management, secure default configuration, protection of data confidentiality (e.g. by encryption) and integrity, process availability and limitation of attack surfaces
Manufacturers shall handle vulnerabilities, including:	Identify vulnerabilities, provide security updates, perform regular tests, publicise information about *fixed* vulnerabilities
'Important products with digital elements', such as:	Operating systems, identity and access management systems, network management systems, microprocessors, microcontrollers, IDS, IPS, routers and firewalls
'Critical products with digital elements'	Includes smart meter gateways

Supervision of critical-impact entities

Additional means of supervision – only for critical-impact entities

Demonstration of compliance

Competent Authorities may request entities to demonstrate their compliance with the NCCS cybersecurity management system and controls.

National verification schemes

Competent Authorities may establish them to verify the implementation of controls, standards and technical specifications (‘mapping matrix’).

May be based on an inspection by the Competent Authority, independent security audits or on mutual peer reviews by critical-impact entities supervised by the Competent Authority.

Cyber-attacks, threats and vulnerabilities

Reportable cyber-attacks

If a Competent Authority receives such information...

Share it with CSIRTs and Competent Authorities in other Member States	Within 24 hours and provide updates. Also try to correlate the information.
Share with other entities within that Member State so they can defend themselves	Within 24 hours, after anonymising and removing business secrets. Provide updates.
May request that entity to share it with other entities that may be affected	To generate situational awareness and to prevent a cross-border cybersecurity electricity incident

Threats and vulnerabilities

If a Competent Authority receives information related to...

Cyber threat	Forward it to the CSIRT
Unpatched actively exploited vulnerability	Forward it to the CSIRT in the Member State where the vulnerability has been reported In coordination with its CSIRTs, share any mitigation strategies

Member State cybersecurity risk assessment

Member State cybersecurity risk assessment – every three years

Primary inputs	Outputs for the Member State report
High-impact and critical-impact entities' risk assessment reports	Implementation status of the cybersecurity controls
Risk preparedness plan under Art. 10 of Electricity Risk Preparedness Regulation	All cyber-attacks and summary of cyber threat information reported in the previous three years
	For each Union-wide HI/CI process, risk estimate for information and related assets

Aggregate the information and submit the Member State risk assessment report to the ENTSO-E and the EU DSO entity

Main tasks of NRAs if designated as Competent Authorities under Risk Preparedness Regulation 2019/941

Risk Preparedness Regulation 2019/941

Main tasks of NRAs if designated as Competent Authorities for Risk Preparedness

Assess all risks to security of electricity supply (Art. 4)	Cooperate with TSOs, DSOs, NRAs, ENTSO-E and RCCs
Identify national electricity crisis scenarios (Art. 7)	Consistent with main risks identified under Reg 2019/941 and with regional electricity crisis scenarios identified by ENTSO-E (Art. 6)
Establish risk-preparedness plans (Art. 10)	Based on national and regional electricity crisis scenarios Consists of national, bilateral and regional bilateral measures
Recital 7, second sentence	Ensure that cyber-incidents are properly identified as a risk, and that the countermeasures are properly reflected in the risk-preparedness plans

Art. 10 Risk-preparedness plan

NATIONAL MEASURES	REGIONAL AND BILATERAL MEASURES
Responsibilities of the competent authority	Crisis coordinator
National measures mitigating risks identified in national and regional crisis scenarios	Cooperation and information sharing mechanisms
National crisis coordinator and its tasks	Coordinated measures to mitigate an electricity crisis
Detailed procedures to be followed, including information flows	Procedures for carrying out annual or biennial tests of the risk-preparedness plans
Market and non-market measures	Triggers for non-market-based measures
Framework for manual load shedding	

Going back to the tasks of the NCCS Competent Authorities...

National cybersecurity crisis management and response plan

Article 41(2) of the NCCS

‘(...) each competent authority shall develop a national cybersecurity crisis management and response plan for cross-border electricity flows taking into account:

- the **Union-level cybersecurity crisis management plan** [established by ACER prior to that] and
- the **national risk preparedness plan established** in accordance with Article 10 of Regulation (EU) 2019/941.’

Cross-border crisis management

If an electricity crisis is related to a cyber-attack impacting more than one Member State...

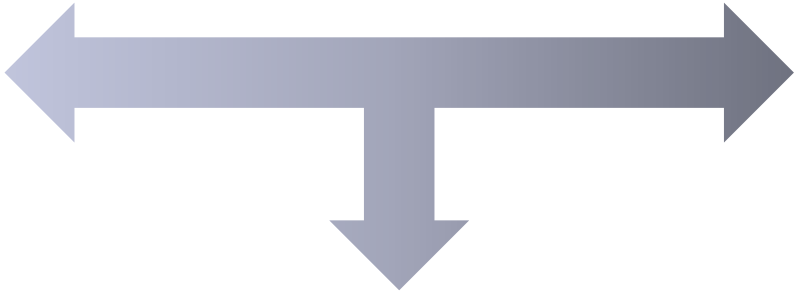
Create an ad hoc cross-border crisis coordination group	Consisting of the NCCS Competent Authorities, Cybersecurity Authorities, Cyber Crisis Management Authorities and Risk Preparedness Authorities
This ad hoc group shall:	Coordinate retrieval and dissemination of information to the entities involved Organise communication between the entities and the competent authorities In cooperation with the CSIRTs, assist the entities with mitigation
Large-scale cybersecurity incident?	Additionally, inform and support the EU CyCLONe

CyCLONe
European Cyber Crises Liaison Organisation Network

Cybersecurity exercises, every three years

Each critical-impact entity

or, instead...



Risk Preparedness Competent Authority may organise at Member State level

Either way, lessons learned

Monitoring cooperation with ACER

Article 17 of the NCCS

ACER, in cooperation with each NCCS Competent Authority, shall monitor:

- implementation of cybersecurity risk management measures by the entities
- reporting of risk assessments by the entities
- reporting of cyber-attacks and threats by the entities
- adoption and implementation progress of the TCMPs

Temporary provisions

Temporary provisions

Tasks of the Competent Authorities in the provisional period

By 13 September 2024	Provide a list of national legislation with relevance for cybersecurity aspects of cross-border electricity flows to the ENTSO-E and the EU DSO entity
By 13 February 2025	Identify candidates for HI/CI entities
By 13 March 2025	Notify the candidates

Thank you

slawomir.bryska@acer.europa.eu