entsoe EU DSO entity

Network Code for cybersecurity aspects of cross-border electricity flows

28 October 2021

This document is a draft network code for cybersecurity aspects of cross-border electricity flows (Network Code) released for public consultation in accordance with the provisions of the Article 31 of Regulation (EU) 2019/943.

The document reflects the status of the work of ENTSO-E and EU DSO entity experts as of 28 October 2021 in line with the ACER Framework Guidelines on sector-specific rules for cybersecurity aspects of cross-border electricity flows dated 28 July 2021. The Network Code also reflects the comments received from the Drafting Committee established pursuant to Article 59(10) of the Regulation (EU) 2019/943.

The document does not in any case represent a firm, binding or definitive ENTSO-E or EU DSO entity position on the content, the structure or the prerogatives of the Network Code.

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity and in particular Article 59(2)(e) thereof,

Whereas:

(1) Sound cybersecurity requirements are crucial for maintaining security of electricity supply and ensure the highest level of cybersecurity protection in the electricity sector.

(2) Energy technologies embedding digital components and the security of the associated supply chains are important for the continuity of essential services and for the strategic control of critical energy infrastructure. This Regulation will therefore contribute actively to the strategic objectives set in the "Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade" (JOIN(2020) 18 final).

(3) Directive (EU) 2016/1148 of the European Parliament and of the Council lays down general rules on security of network and information systems. Regulation (EU) 2019/941 complements Directive (EU) 2016/1148 by ensuring that cyber-incidents are properly identified as a risk, and that the measures taken to address them are properly reflected in the risk-preparedness plans. Regulation (EU) 2019/943 complements Directive (EU) 2016/1148 and Regulation (EU) 2019/941 by providing for sector-specific rules at Union level.

(4) Regulations (EU) 2019/943 in Art. 59(2)(e) empowers the Commission to adopt delegated acts on sector-specific rules at Union level for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management.

(5) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on the European Union Agency for Cybersecurity ('ENISA') and on information and communications technology cybersecurity certification recognizes the vital role of the energy sector for the economy and provides for ENISA to liaise with the Agency for the cooperation of energy regulators ('ACER').

(6) Regulation (EU) 2019/943 assigns specific responsibilities with regard to cybersecurity to Transmission System Operators ('TSOs') and Distribution System Operators ('DSOs') and their European associations the ENTSO for Electricity and the EU DSO entity shall promote cybersecurity in cooperation with relevant authorities and regulated entities.

(7) The provisions of this Regulation should be without prejudice to Union law providing specific rules on the certification of ICT products, ICT services and ICT processes, in particular without prejudice to the provisions laid down in Article 46 of Regulation (EU) 2019/881 with regard to the framework for the establishment of European cybersecurity certification schemes.

(8) Technology is evolving constantly and digitalization of the electricity sector is progressing rapidly. This Regulation shall not be detrimental to innovation and not constitute a barrier to the access of new electricity entities to the electricity market and the subsequent use of innovative solutions that contribute to the efficiency of the electricity system.

(9) The monitoring of the implementation of this Regulation shall limit the collection of

information to a reasonable amount, shall provide achievable and effective deadlines for stakeholders to submit such information and avoid double notification by the concerned critical-impact and high-impact entities and their associations.

(10) Cybersecurity protection does not stop at the Union's borders. A secure system requires the involvement of neighbouring third country parties. The Union, its Members States, national institutions, TSOs and DSOs shall support neighbouring third countries in applying similar cybersecurity rules as set out in this Regulation. The ENTSO for Electricity and the EU DSO entity shall facilitate cooperation between the Union TSOs and DSOs and neighbouring third country TSOs and DSOs.

(11) This Regulation has been developed in close cooperation with ACER, ENISA, the ENTSO for Electricity, the EU DSO entity and stakeholders, in order to adopt effective, balanced and proportionate rules in a transparent and participative manner. In accordance with Article 60 of Regulation (EU) 2019/943 the Commission, ACER, the ENTSO for Electricity and the EU DSO entity will follow the procedure and consultation obligations set out in Article 59 of Regulation (EU) 2019/943 before proposing any amendment to this Regulation.

HAS ADOPTED THIS REGULATION:

TITLE I
GENERAL PROVISIONS

Article 1 Subject Matter

This Regulation establishes a network code, which lays down sector-specific rules for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management.

Article 2 Scope

1. The provisions set out in this Regulation shall apply to the following entities:

   (a) electricity undertakings as defined in Article 2(57) of Directive (EU) 2019/944;

   (b) NEMOs as defined in Article 2(7) and (8) of Regulation (EU) 2019/943;

   (c) electricity digital market platforms as defined in Article 4(29);

   (d) critical service providers as defined in Article 4(9);

   (e) Regional Coordination Centres (RCCs) established pursuant to Article 35 of Regulation (EU) 2019/943;

   (f) the ENTSO for Electricity as defined in Article 24 of Regulation (EU) 2019/943;

   (g) the European Network of Distribution System Operators for Electricity (‘EU DSO entity’) as defined in Article 52 of Regulation (EU) 2019/943;

(h) the Agency for the Cooperation of Energy Regulators ('ACER') as defined in Regulation (EU) 2019/942;

(i) national regulatory authorities ('NRAs') as defined in Article 59 of Directive (EU) 2019/944;

(j) national competent authorities for risk preparedness ('RP-NCA') as defined in Article 3 of Regulation (EU) 2019/941;

(k) cybersecurity operation centre ('CSOCs') as defined in Article 4(16);

(l) national competent authorities for cybersecurity ('CS-NCA') as defined in Article 8 of Directive (EU) 2016/1148;

(m) Computer Security Incident Response Teams ('CSIRTs') as defined in Article 9 of Directive (EU) 2016/1148;

(n) the European Union Agency for Cybersecurity ('ENISA') as defined in Regulation (EU) 2019/881;

(o) and any entity or third party to whom responsibilities have been delegated or assigned with a relevant cybersecurity impact on the cross-border electricity flow.

2. This Regulation shall not apply to a micro or small sized enterprise, or any other entity not listed in Article 2 (1), unless one or more of the following conditions are fulfilled:

(a) application is requested by any entity listed in Article 2 (1);

(b) application is requested by the Commission;

(c) the micro or small sized enterprise, or any other entity, is classified as a critical-impact or high-impact entity in accordance with the electricity cybersecurity impact index developed under Article 19.

The NRAs and the CS-NCAs shall jointly decide whether the application request pursuant to (2)(a) and (b) is admissible and keep a list of the micro and small sized enterprises or any other entity that fulfil the conditions 2(a) and (b).

3. Notwithstanding any other provision of this Regulation, a micro or small sized enterprise and any other entity not listed in Article 2 (1), not classified as a critical-impact or high-impact entity, shall implement the basic cybersecurity hygiene requirements as defined in Annexe A within 12 months after entry into force of this Regulation.

4. This Regulation shall apply to critical service providers not established in the Union but that deliver services to entities in the Union. Where such a critical service provider delivers data processing services, large-scale services and regular services to electricity entities established in the Union, this critical service provider shall explicitly designate a representative established in the Union to act on behalf of this critical service provider. This representative may be addressed by any competent authority in the Union instead of the critical service provider with regard to obligations of that critical service provider under this Regulation. The representative will be subject to enforcement proceedings in the event of non-compliance by that critical service provider with this Regulation.

Article 3 **Objectives**

1. This Regulation aims at:

   (a) establishing a solid governance for cybersecurity aspects of cross-border electricity flows to ensure the reliability of the energy system and to ensure close collaboration with existing governance structure(s) for cybersecurity;

   (b) determining common criteria for risk assessment to identify risk scenarios for the operational reliability of the electricity system with regard to cross-border ;;

   (c) promoting a common electricity cybersecurity framework and by that fostering a common minimum electricity cybersecurity level across the Union;

   (d) providing for clear verification rules by a third party in order to assess the application of the minimum and advances cybersecurity controls;

   (e) establishing essential information flows by setting up a system for the collection and sharing of essential information in relation to cross-border electricity flows;

   (f) establishing effective processes to identify, classify and respond to cross-border cybersecurity incidents;

   (g) setting up effective processes for crisis management to handle cybersecurity incidents of cross-border relevance;

   (h) defining common principles for electricity cybersecurity exercises to increase the risk preparedness of the electricity sector;

   (i) protecting the information exchanged in the context of data processing;

   (j) determining a process to monitor the implementation of this Regulation, to assess the effectiveness of the investments in cybersecurity protection and to report on the progress in cybersecurity protection across the Union;

   (k) ensuring that the cybersecurity procurement requirements with relevance for cross-border electricity flows are not detrimental to innovation, new systems, processes and procedures.

2. When applying this Regulation, Member States, competent authorities and regulatory authorities, transmission system operators and distribution system operators shall:

   (a) apply the principles of proportionality and non-discrimination;

   (b) ensure transparency;

   (c) respect the responsibility assigned to the relevant TSO and DSO in order to ensure system security, including as required by national legislation;

   (d) consult with relevant stakeholders and take account of potential impacts on their systems; and

   (e) take into consideration agreed Union standards and technical specifications;

   (f) avoid double reporting and strive to reduce additional administrative burden on all involved entities.

Article 4 **Definitions**

For the purpose of this Regulation, the definitions in Article 2 of Regulation (EU) 2019/943, the definitions in Article 2 of Directive (EU) 2019/944, the definitions in Article 4 of Directive (EU) 2016/1148, the definitions in Article 2 of Regulation (EU) 2019/941, the definitions in Article 2 of Regulation (EU) 2019/881 shall apply.

The following definitions shall also apply:

(1) 'asset' means anything that has value to the organization, including business processes, information, hardware, software, networks and sites;

(2) 'classified information' means information considered to be classified in accordance with Union or national legislation;

(3) 'competent authorities for cybersecurity' or 'CS-NCAs' means all national competent authorities responsible for the implementation, monitoring and supervision of cybersecurity at Member State level as defined in accordance with Article 8 of Directive (EU) 2016/1148;

(4) 'competent authorities for risk preparedness' or 'RP-NCAs' means the competent national authority as defined in Article 3 of Regulation (EU) 2019/941.

(5) 'computer security incident response team (CSIRT)' means a team responsible for risk and incident handling in accordance with Article 9 of Directive (EU) 2016/1148;

(6) 'conformity assessment body' means a body that performs conformity assessment activities including calibration, testing, certification and inspection;

(7) 'critical-impact asset' means an asset needed for a critical-impact process

(8) 'critical-impact electricity crisis' means a present or imminent situation in which there is a significant electricity shortage, as determined by the Member States and described in their risk-preparedness plans, or in which it is impossible to supply electricity to customers;

(9) 'critical-impact entity' means an electricity entity that has a critical-impact process;

(10) 'critical-impact perimeter' means a logical and physical perimeter defined by an entity that contains all critical-impact asserts and on which access to these assets can be controlled; the critical-impact perimeter defines the scope where the advanced cybersecurity controls apply;

(11) 'critical-impact process' means a business process for which the electricity cybersecurity impact indices are above the critical-impact threshold;

(12) 'critical-impact threshold' means the values of the electricity cybersecurity impact indices, defined by the ENTSO for Electricity and the EU DSO entity above which a process will cause disruption of cross-border electricity flows;

(13) 'critical service provider' means a natural or legal person who operates or provides any critical service directly or on behalf of an entity;

(14) 'cross border electricity crisis' means an incident with electric effects on more than one Member State, and one or more of the affected TSOs classify the electricity incident as a Scale 2 or 3 incident according to the Incident Classification Scale Methodology of the ENTSO for Electricity;

(15) 'cross-border electricity flow' means a physical flow of electricity on a transmission network

of a Member State that results from the impact of the activity of producers, customers or both, outside that Member State on its transmission network as defined in point (3) of Article 2 of Regulation (EU) 2019/943;

(16) ‘cyber-attack’ means any attempt with malicious intent to gain access to network and information systems. A cyber-attack may cause an incident where damages, disruptions or dysfunctionalities occur;

(17) ‘cybersecurity’ means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats;

(18) ‘cybersecurity cross-border crisis’ means a cross-border electricity crisis that is caused partially or totally by a cybersecurity root cause;

(19) ‘cybersecurity operation centre (CSOC)’ means an entity staffed with one or more IT and/or OT staff who perform security related tasks such as log analysis, incident detection, incident handling and security configuration;

(20) ‘cybersecurity posture’ means the overall cybersecurity status of an organisation including procedures, processes, skills, tools and resources to defend proactively and reactively against cyber-attacks;

(21) ‘cybersecurity procurement requirements’ means the requirements that entities define for new or updated ICT products, ICT processes or ICT services during procurement;

(22) ‘cyber threat’ means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons;

(23) ‘cyber threat actor‘ means any individual or group, deliberately or not deliberately, and consciously or unconsciously, contributing to the existence of a cyber-threat;

(24) ‘distribution system operator’ means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the distribution system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the distribution of electricity as defined in point (29) of Article 2 of Directive (EU) 2019/944;

(25) ’early cyber warning’ means a provision of concrete information indicating the possible existence of a cyber-threat;

(26) ’early cyber warning system’ means a solution for gathering, processing and notifications of early cyber warnings;

(27) ‘electricity cybersecurity impact index(es)’ means the indices defined by the cybersecurity risk working group for business processes of the electricity sector to estimate the possible consequences of cyber-attacks to cross-border electricity flows;

(28) ‘electricity cybersecurity perimeter’ means a logical and physical perimeter defined by an entity that contains all assets needed for Union-wide high-impact and critical-impact processes and on which access to these assets can be controlled; the electricity cybersecurity perimeter defines the scope of the cybersecurity risk assessment at entity level;

(29) ‘electricity digital market platform’ means a digital platform for electricity market data management and electricity trading;

(30) ‘electricity entity‘ means electricity undertakings as defined in Article 2(57) of Directive (EU) 2019/944, NEMOs, electricity digital market platforms, regional coordination centres (RCCs), the ENTSO for Electricity, the EU DSO entity, ACER, NRAs, RP-NCAs, CSOCs, CS-NCAs and CSIRTs;

(31) ‘European cybersecurity certification scheme’ means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes;

(32) ‘high-impact asset’ means any asset needed for a high-impact process;

(33) ‘high-impact entity’ means an electricity entity that has a high-impact process;

(34) ‘high-impact perimeter’ means a logical and physical perimeter defined by an entity that contains all high-impact assets and on which access to these assets can be controlled; the high-impact perimeter defines the scope where the minimum cybersecurity controls apply;

(35) ‘high-impact process’ means any business process for which the electricity cybersecurity impact indices are above the high-impact threshold;

(36) ‘high-impact threshold’ means the values of the electricity cybersecurity impact indices defined by the ENTSO for Electricity and the EU DSO entity above which a process could cause disruption of cross-border electricity flows;

(37) ‘ICT product‘ means an element or a group of elements of a network or information system;

(38) ‘ICT process’ means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service;

(39) ‘ICT service’ means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems;

(40) ‘incident’ means any event having an actual adverse effect on the security of network and information systems;

(41) ‘information and communication technology’ or ‘ICT’ means information being processed digitally in information technology systems and transferred across communications networks;

(42) ‘legacy systems’ means an obsolete network and information system that cannot be modified or updated to meet minimum cybersecurity requirements. Legacy system also includes hardware and/or software systems that cannot be protected by other means without causing damages, disruptions or dysfunctionalities to operations linked to electricity cross-border flows;

(43) ‘likelihood’ means the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically such as a probability or a frequency over a given time period, in accordance with ISO Guide 73:2009, definition 3.6.1.1;

(44) ‘Managed Security Service Provider’ or ‘MSSP’ means a provider of CSOC services for an entity who lacks such capabilities itself and/or prefers to outsource such services;

(45) ‘network and information system’ means: (a) an electronic communications network within

the meaning of Article 2(a) of Directive 2002/21/EC; (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;

(46) 'NIS Cooperation Group' means a group with a mission to achieve a high common level of security for network and information systems (NIS) in the Union as described in Article 11 of Directive (EU) 2016/1148. It supports and facilitates the strategic cooperation and the exchange of information among Member States. The NIS Cooperation Group is composed of representatives of the Member States, the Commission and ENISA;

(47) 'operational technology' or 'OT' means the use of computers and data networks to operate physical systems.

(48) 'originator' means an entity that initiates an information exchange, information sharing or information storage event;

(49) 'regulatory authority' or 'NRA' means a regulatory authority designated by each Member State pursuant to Article 57(1) of Directive (EU) 2019/944.

(50) 'transmission system operator' means a natural or legal person who is responsible for operating, ensuring the maintenance of and, if necessary, developing the transmission system in a given area and, where applicable, its interconnections with other systems, and for ensuring the long-term ability of the system to meet reasonable demands for the transmission of electricity as defined in point (35) of Article 2 of Directive 2019/944;

(51) 'Union cybersecurity certification scheme' means a comprehensive set of rules, technical requirements, standards and procedures that are established at Union level and that apply to the certification or conformity assessment of specific ICT products, ICT services or ICT processes;

(52) 'Union-wide critical-impact process' means any electricity sector process, possibly involving multiple entities, for which the possible impact of a compromise is evaluated as critical during the Union-wide risk assessment;

(53) 'Union-wide high-impact process' means any electricity sector process, possibly involving multiple entities, for which the possible impact of a compromise is evaluated as high during the Union-wide risk assessment;

(54) 'penetration testing' means an authorized simulated cyber-attack on a computer system, performed to evaluate the security of the system. Penetration testing shall cover known and emerging vulnerabilities, and consider the system becoming unavailable also through non-malicious actions;

(55) 'real-time system' means a system in which its temporal properties are essential for reliability and correctness;

(56) 'regional coordination centre" means regional coordination centre established pursuant to Article 35 of Regulation (EU) 2019/943

(57) 'representative' means any natural or legal person established in the Union explicitly designated to act on behalf of a digital service provider not established in the Union, which

may be addressed by a national competent authority or a CSIRT instead of the digital service provider with regard to the obligations of that digital service provider under this Regulation;

(58) 'risk impact matrix' or 'RIM' means a matrix used during risk assessment to describe the resulting risk impact level for each risk assessed;

(59) 'sensitive non-classified information' means information or material that the entities defined in Article 2, Title 10 of this Regulation, must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof, and/or because of its sensitivity;

(60) 'simultaneous electricity crisis' means an electricity crisis affecting more than one Member State at the same time;

(61) 'system operation regions' means the system operation regions as defined in accordance with Article 36 of Regulation (EU) 2019/943 on the geographical scope of regional coordination +centres;

(62) 'vulnerability' means a weakness, susceptibility or flaw of an ICT asset or a system that can be exploited by a cyber-threat;

(63) '0 days vulnerability' means a vulnerability, in ICT asset, that was not spotted during the testing phase and has been discovered by at least one person but has not yet been publicly announced or patched.

Article 5 Adoption of methodologies

1. The ENTSO for Electricity in cooperation with the EU DSO entity shall develop the methodologies required by this Regulation and submit them for approval to ACER or the competent regulatory authorities within the respective deadlines set out in this Regulation. In exceptional circumstances, notably in cases where a deadline cannot be met due to circumstances external to the sphere of ENTSO for Electricity in cooperation with the EU DSO entity the deadlines for methodologies may be prolonged by ACER in procedures pursuant to paragraph 5, jointly by all competent regulatory authorities in procedures pursuant to paragraph 6.
2. The ENTSO for Electricity and the EU DSO entity shall regularly inform the competent regulatory authorities and ACER about the progress of developing those methodologies.
3. If the ENTSO for Electricity in cooperation with the EU DSO entity fails to submit an initial or amended proposal for methodologies to the competent regulatory authorities or ACER in accordance with paragraphs 5 and 6 within the deadlines set out in this Regulation, they shall provide the competent regulatory authorities and ACER with the relevant drafts of the proposals for the methodologies and explain what has prevented an agreement. ACER, all competent regulatory authorities jointly, or the competent regulatory authority shall take the appropriate steps for the adoption of the required methodologies in accordance with paragraphs 4 and 5 respectively, for instance by requesting amendments or revising and completing the drafts pursuant to this paragraph, including where no drafts have been submitted, and approve them.
4. The proposals for the following methodologies and any amendments thereof shall be subject to approval by ACER:

   (a) the cybersecurity risk assessment methodologies pursuant to Article 17(1);

   (b) the methodology to determine the high-impact and critical-impact perimeters pursuant to

Article 17(3);

(c) the cross-border electricity cybersecurity risk assessment report pursuant to Article 22;

(d) the common electricity cybersecurity framework pursuant to Article 23;

(e) the harmonised cybersecurity procurement requirements pursuant to Article 35;

(f) the cybersecurity incidents classification scale methodology pursuant to Article 36;

5. The proposals for the following methodologies and any amendments thereof shall be subject to approval by all regulatory authorities of the concerned system operation region:

   (a) the regional risk treatment plans pursuant to Article 20.

6. The proposal for methodologies shall include a proposed timescale for their implementation and a description of their expected impact on the objectives of this Regulation. Proposals for methodologies subject to the approval by several regulatory authorities in accordance with paragraph 5 shall be submitted to ACER within 1 week of their submission to regulatory authorities. Upon request by the competent regulatory authorities, ACER shall issue an opinion within 3 months on the proposals for methodologies. Upon request by ACER, the Commission shall issue an opinion within 3 months on the proposals for methodologies.

7. Where the approval of the methodologies in accordance with paragraph 6 or the amendment in accordance with paragraph 9 requires a decision by more than one regulatory authority, the competent regulatory authorities shall consult and closely cooperate and coordinate with each other in order to reach an agreement. Where applicable, the competent regulatory authorities shall take into account the opinion of ACER. Regulatory authorities or, where competent, ACER shall take decisions concerning the submitted methodologies in accordance with paragraphs 4 and 5, within 6 months following the receipt of the methodologies by ACER or the regulatory authority or, where applicable, by the last regulatory authority concerned. Upon request by ACER, the Commission shall issue an opinion within 3 months on the proposals for methodologies. Where applicable, ACER shall take into account the opinion of the Commission. The period shall begin on the day following that on which the proposal was submitted to ACER in accordance with paragraph 4, to the last regulatory authority concerned in accordance with paragraph 6.

8. Where the regulatory authorities have not been able to reach agreement within the period referred to in paragraph 8, or upon their joint request, or upon ACER's request according to the third subparagraph of Article 5(3) of Regulation (EU) 2019/942, ACER shall adopt a decision concerning the submitted proposals for methodologies within 6 months, in accordance with Article 5(3) and the second subparagraph of Article 6(10) of Regulation (EU) 2019/942.

9. In the event that ACER, or all competent regulatory authorities jointly, or the competent regulatory authority request an amendment to approve the methodologies submitted in accordance with paragraphs 4 and 5 respectively, the ENTSO-E for Electricity in cooperation with the EU DSO entity shall submit a proposal for amended methodologies for approval within 2 months following the request from ACER or the competent regulatory authorities or the competent regulatory authority. ACER or the competent regulatory authorities or the competent regulatory authority shall decide on the amended methodologies within 2 months following their submission. Where the competent regulatory authorities have not been able to reach an agreement on methodologies

pursuant to paragraph 6 within the 2-month deadline, or upon their joint request, or upon ACER's request according to the third subparagraph of Article 5(3) of Regulation (EU) 2019/942, ACER shall adopt a decision concerning the amended methodologies within 6 months, in accordance with Article 5(3) and the second subparagraph of Article 6(10) of Regulation (EU) 2019/942. If the ENTSO for Electricity fails to submit a proposal for amended methodologies, the procedure provided for in paragraph 3 of this Article shall apply.

10. ACER, or all competent regulatory authorities jointly, or the competent regulatory authority, where they are responsible for the adoption of methodologies in accordance with paragraphs 4 and 5 may respectively request proposals for amendments of those methodologies and determine a deadline for the submission of those proposals. The ENTSO for Electricity in cooperation with the EU DSO entity may propose amendments to regulatory authorities and ACER.

    The proposals for amendment to the methodologies shall be submitted to consultation in accordance with the procedure set out in Article 8 and approved in accordance with the procedure set out in this Article.

11. The ENTSO for Electricity in cooperation with the EU DSO entity responsible for establishing the methodologies in accordance with this Regulation shall publish them on the internet after approval by ACER or the competent regulatory authorities or, if no such approval is required, after their establishment, except where such information is considered as confidential in accordance with Article 6 and 7.

Article 6 Publication of methodologies on the internet

1. The ENTSO for Electricity and the EU DSO entity shall publish the methodologies on the internet following approval by ACER or the competent NRAs or, where no such approval is required, following their specification, except where such information is considered confidential in accordance with Articles 10 and 11.
2. The publication shall also concern all methodologies listed in Article 5(4) and (5).

Article 7 Stakeholder involvement

1. The ENTSO for Electricity and the EU DSO entity, shall organise stakeholder involvement via the Working Group pursuant to Article 15. This shall include regular meetings with stakeholders to identify problems and propose improvements related to the implementation of this Regulation. This shall not replace the stakeholder consultations in accordance with Article 8.
2. The ENTSO for Electricity in coordination with the EU DSO entity shall inform the Electricity Coordination Group on the proposals for the cybersecurity risk assessment methodologies.
3. ACER shall organise involvement of other competent authorities at Union and national level via the Monitoring Body pursuant to Article 16. This shall include regular meetings with the authorities to identify problems and propose improvements notably related to monitoring of the implementation of this Regulation.
4. ACER shall consult ENISA before adopting or amending the proposals listed in Article 5 (4).

Article 8 Public consultation

1. The ENTSO for Electricity and the EU DSO entity shall consult stakeholders, including ACER, ENISA and the NRAs of each Member State, on the draft proposals for methodologies listed in Article 5 (4). The consultation shall last for a period of not less than one (1) month.
2. The proposals for methodologies submitted by the ENTSO for Electricity and the EU DSO entity at Union level shall be published and submitted to public consultation at Union level. Proposals submitted by the ENTSO for Electricity and the EU DSO entity at regional level shall be submitted to public consultation at least at regional level.
3. The ENTSO for Electricity and the EU DSO entity shall duly take into account the views of stakeholders resulting from the consultations prior to its submission for regulatory approval. In all cases, a sound justification for including or not including the views resulting from the consultation shall be provided together with the submission of the proposal and published in a timely manner before, or simultaneously with the publication of the proposal for methodologies.

Article 9 Recovery of costs

1. The costs borne by transmission system operators and distribution system operators subject to network tariff regulation and stemming from the obligations laid down in this Regulation shall be assessed by the relevant regulatory authorities. Costs assessed as reasonable, efficient and proportionate shall be recovered through network tariffs or other appropriate mechanisms.
2. If requested by the relevant regulatory authorities, transmission system operators and distribution system operators referred to in paragraph 1 shall, within 3 months of the request, provide the information necessary to facilitate assessment of the costs incurred.

Article 10 Confidentiality obligation

1. Any confidential information received, exchanged or transmitted pursuant to this Regulation shall be subject to the conditions of professional secrecy laid down in paragraphs 2, 3 and 4. All information exchanged among entities listed in the Article 2, for the purposes of implementing this Regulation, shall be protected, considering the level of classification of the information applied to the information by the sender.
2. The obligation of professional secrecy shall apply to any entities subject to the provisions of this Regulation.
3. Confidential information received by any entities or authorities referred to in paragraph 2 in the course of their duties may not be divulged to any other entities or authority, without prejudice to cases covered by national law, other provisions of this Regulation or other relevant Union legislation.
4. Without prejudice to cases covered by national or Union legislation, an authority, entity or natural person who receives confidential information pursuant to this Regulation may not use it for any other the purpose than carrying out its duties under this Regulation.

Article 11 Information Confidentiality Classification and Protection

1. All entities referred to in Article 2 of this Regulation are responsible for the classification of their

information as sensitive non classified information or EU classified information defined as follows:

(a) confidential: information and material the unauthorised disclosure of which could harm the essential interest of the data originator.

(b) sensitive: information and material the unauthorised disclosure of which could be disadvantageous the essential interest of the data originator.

2. The classification of information shall abide by the classification system set in Title X of this Regulation, and in accordance with the principle in recital 8 set out in Directive (EU) 2016/1148 and without prejudice to any other relevant Union legislation.

3. All information exchanged between entities shall be protected accordingly to the level of classification of the information itself and systems used to protect the information shall conform with the security measures foreseen to implement such protection.

Article 12 Monitoring

1. ACER shall monitor the implementation of this Regulation in accordance with Article 32(1) of Regulation (EU) 2019/943. ACER shall carry out the monitoring activities in cooperation with ENISA and with the support of the ENTSO for Electricity and the EU DSO entity. ACER shall regularly inform the Electricity Coordination Group on the implementation of this Regulation.

2. The monitoring shall take place at least every two (2) years and shall:

(a) assess the contribution of the measures implemented to the three (3) key objectives set out in the "Joint Communication to the European Parliament and the Council - The EU's Cybersecurity Strategy for the Digital Decade" (JOIN(2020) 18 final);

(b) verify the status of implementation of the applicable cybersecurity standards, with regard to the high-impact and critical-impact entities, with a priority focus on the high-impact entities;

(c) verify whether the size cap does not directly or indirectly cause a systemic cybersecurity risk for cross-border electricity flows;

(d) identify whether additional measures to the ones laid out in this Regulation may be necessary to prevent risks for the electricity sector;

(e) identify areas of improvement for the revisions of this Regulation, or to determine uncovered areas and new priorities that may emerge due to technological advances.

3. ACER, in cooperation with ENISA shall establish within 12 months from the entry into force of this Regulation the methodology and rules to collect the relevant information to be communicated to ACER in accordance with Regulation (EU) 2019/943. ACER shall then consult the ENTSO for Electricity and the EU DSO entity on the methodology. The methodology and rules for the collection of such information may be subject to updates by ACER, the ENTSO for Electricity and the EU DSO entity. ACER, the ENTSO for electricity and the EU DSO entity shall agree on a reasonable timeframe to update such information and on common standardised ways of analysing the information.

4. NRAs and CS-NCAs shall have access to relevant information held by ACER, which it has collected in accordance with this Article.

5. ACER shall determine in cooperation with ENISA and with the support of the ENTSO for

Electricity and the EU DSO entity performance indicators that allow assessing operational reliability that can be related to cybersecurity aspects of cross-border electricity flows.

6. The entities listed in Article 2(1) of this Regulation shall submit to ACER the information required to perform the tasks referred to in paragraph 1.

Article 13 Benchmarking

1. Within 12 months after entry into force of this Regulation

   (a) ACER, in cooperation with ENISA, shall establish a non-binding cybersecurity benchmarking guide.

   (b) ACER shall provide target values, based on existing reports, which shall make the basis of the non-binding cybersecurity benchmarking guide.

   (c) ACER shall submit the non-binding cybersecurity benchmarking guide to the NRAs.

2. Taking into account the non-binding benchmarking guide, the NRAs shall carry out a benchmarking to assess whether current investments in cybersecurity to mitigate risks having an impact on cross-border electricity flows provide the desired results and what are the efficiency gains for the development of the electricity systems; and whether such investments are efficient and integrated into the overall procurement of assets and services.

3. The NRAs shall assess in the benchmarking in particular:

   (a) the average expenditure in cybersecurity for mitigating risks having an impact on electricity cross-border flows, especially in respect to the high-impact entities and to the critical-impact entities;

   (b) the average expenditure on the fulfilling of the basic cyber hygiene requirements for all the entities which are not high-impact or critical-impact entities;

   (c) in coordination with RCCs, the average prices of cybersecurity services, systems and products that mainly contribute to the enhancement and maintenance of the cybersecurity posture in the different system operation regions; to allow to analyse the existence of similar costs associated with cybersecurity as well as to identify possible measures needed to foster efficiency in spending, particularly where cybersecurity technological investments may be needed;

   (d) the level of efficiency of spending on cybersecurity and observe the correlation between the level of spending and the maturity of the sector (prudence of cybersecurity expenditure). To know whether a security measure is cost efficient, the costs of the measure shall be compared with the economic impact of a cyber-incident in case the measure is not in place. To find the cost of the measure, the price of operating a service without cyber measures and cyber-attacks may be compared with the price of operating a service which includes security systems. To enable such a comparison, security costs shall be separated from other investment costs and operations costs.

4. Any information related to cybersecurity spending shall remain sensitive information and shall be managed jointly and securely by the CS-NRAs and NRAs with national security clearances at the Member State level and ACER and ENISA at the Union level. If an NRA has no security clearances at Member State level, the CS-NCA will grant the NRA relevant access to classify information on

a “need to know” basis. These potential situations shall be described in the Cross-Border Electricity Cybersecurity Assessment Report.

5. The benchmarking pursuant to paragraphs 2 and 3 shall not be made public.

Article 14 Agreements with TSOs and DSOs not bound by this Regulation

Within 18 months after entry into force of this Regulation, all TSOs and DSOs of a system operation region that is neighbouring to a third country shall endeavour to conclude with the third country TSO(s) and DSO(s) not bound by this Regulation agreements setting the basis for their cooperation concerning secure cybersecurity protection and setting out arrangements for the compliance of the neighbouring third country TSO(s) and DSO(s) with the obligations set out in this Regulation.

TITLE II
GOVERNANCE FOR CYBERSECURITY RISK MANAGEMENT

Article 15 Cybersecurity risk working group

1. Within 1 month after entry into force of this Regulation the ENTSO for Electricity and the EU DSO entity shall

   (a) establish a cybersecurity risk working group (hereafter ‘the Working Group’);

   (b) define the terms of reference for the Working Group;

   (c) co-chair the Working Group.

   The Working Group shall consist of representatives of the ENTSO for Electricity, the EU DSO entity, NEMOs and a limited number of the main affected stakeholders that represent critical-impact and high-impact entities in accordance with Article 2.

2. The Working Group shall support the ENTSO for Electricity and the EU DSO entity in cybersecurity risk assessments, in particular with regard to the following tasks:

   (a) development of the cybersecurity risk assessment methodologies pursuant to Article 17 (1);

   (b) development of the methodology to determine the high-impact and critical-impact perimeters pursuant to Article 17 (3);

   (c) development of the cross-border electricity cybersecurity risk assessment report pursuant to Article 22;

   (d) development of the common electricity cybersecurity framework pursuant to Article 23;

   (e) development of the harmonised cybersecurity procurement requirements pursuant to Article 35;

   (f) development the cybersecurity incidents classification scale methodology pursuant to Article 37(7);

   (g) development the transitional electricity cybersecurity impact index pursuant to Article 49(1);

   (h) development the consolidated transitional list of high impact and critical impact entities pursuant to Article 49(3);

(i) development the transitional list of high-impact and critical-impact processes pursuant to Article 49(4);

(j) development the transitional list of international standards and controls pursuant to Article 49(5).

(k) performance of the Union-wide risk assessment pursuant to Article 19;

(l) performance of the regional cybersecurity risk assessments pursuant to Article 20;

(m) definition of the regional cybersecurity risk treatment plans pursuant to Article 21;

(n) development of guidance on Union verification schemes and Union certification schemes for ICT products, ICT services, and ICT processes in accordance with Article 36.

3. The ENTSO for Electricity and the EU DSO entity shall regularly inform ACER and the Electricity Coordination Group on the implementation steps with regard to the cybersecurity risk assessments.

Article 16 Cybersecurity risk monitoring body

1. Within 3 months after entry into force of this Regulation, ACER shall establish a cybersecurity risk monitoring body (hereafter the 'Monitoring Body').

   The Monitoring Body shall consists of representatives of ACER, ENISA, CS-NCAs, NRAs and RP-NCAs. The Commission may participate as an observer in the Monitoring Body.

2. The Monitoring Body shall support ACER in the following tasks:

   (a) monitoring of the implementation of application of the cybersecurity standards pursuant to Article 12(2)(b);

   (b) adopting the methodologies pursuant to Article 5(4).

Article 17 Cybersecurity risk assessment methodologies

1. Within 9 months after entry into force of this Regulation the ENTSO for Electricity in cooperation with EU DSO entity shall develop proposals for the cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level.

2. The cybersecurity risk assessment methodologies shall include:

   (a) quantitative metrics to measure the consequences of cyber-attacks to cross-border electricity flows taking into account safety, operational security, frequency quality and the efficient use of the interconnected system and resources;

   (b) a list of threats to consider, including at least the following supply chain threats:

      (i) a severe and unexpected corruption of the supply chain;

      (ii) the unavailability of products or services from the supply chain;

      (iii) attacks through actors of the supply chain;

      (iv) supply chain tracking or infiltration.

   (c) criteria to evaluate the consequences and cybersecurity risks as high or critical using a defined threshold for consequences and likelihood;

(d) rules for the definition of the electricity cybersecurity impact index and high-impact and critical-impact thresholds;

(e) an approach to analyse the cybersecurity risks coming from legacy systems, the cascading effects of electricity incidents and the real-time nature of systems operating the grid.

3. Within 9 months after entry into force of this Regulation the ENTSO for Electricity and the EU DSO entity shall develop a methodology for entities to determine their high-impact and critical-impact perimeters building upon their high-impact and critical-impact assets.

4. At least after each cybersecurity risk assessment cycle the ENTSO for Electricity and the EU DSO entity in collaboration with ACER shall review the effectiveness of the cybersecurity risk assessment methodologies. Based on the outcome of that review the ENTSO for Electricity and the EU DSO entity may propose amendments to the cybersecurity risk assessment methodologies.

Article 18 Cybersecurity risk assessment cycle

The cybersecurity risk assessments at Union level, at regional level and at Member State level shall be performed every 2 years. The first risk assessment cycle shall start 18 months after entry into force of this Regulation.

TITLE III
RISK MANAGEMENT AT UNION AND AT REGIONAL LEVEL

Article 19 Union-wide cybersecurity risk assessment

1. The ENTSO for Electricity in cooperation with the EU DSO entity shall perform a cybersecurity risk assessment at Union level to identify, analyse, and evaluate the possible consequences of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. The Union-wide risk assessment shall not consider the legal, financial or reputational damage of cyber-attacks.

2. The Union wide risk assessment report shall include the following elements:

(a) a list of Union-wide high-impact and critical-impact processes;

(b) a risk impact matrix that entities and CS-NCAs shall use to report the cybersecurity risk identified in the Member State cybersecurity risk analysis and the cybersecurity risk assessment at entity level.

3. For Union-wide high-impact and critical-impact processes the cybersecurity risk assessment reports shall include:

(a) an assessment of the possible consequences of a compromise to confidentiality, integrity, or availability of information used in the process using the metrics defined in the Union-wide cybersecurity risk assessment methodology;

(b) a description of the types of entities involved in the Union-wide high-impact and critical-

impact processes;

(c) electricity cybersecurity impact indices and high-impact and critical-impact thresholds that the CS-NCAs can use to identify high-impact and critical-impact entities involved in the Union-wide high-impact and critical-impact processes.

4. Within 6 months after the start of the cybersecurity risk assessment cycle the ENTSO for Electricity in cooperation with the EU DSO entity shall submit the report on the results of the Union-wide cybersecurity risk assessment to ACER for opinion. ACER shall issue an opinion on the report within 3 months after receipt of the draft report. The ENTSO for Electricity in cooperation with the EU DSO entity shall take utmost account of the opinion when finalising the report.

5. The ENTSO for Electricity and the EU DSO entity shall notify the final report to ACER, ENISA, the Commission, the NIS Cooperation Group, the CS-NCAs and NRAs.

Article 20 Regional cybersecurity risk assessments

1. The ENTSO for Electricity in cooperation with the EU DSO entity and with the RCCs shall perform a cybersecurity risk assessment for each system operation region aggregating the Member State cybersecurity risk assessments. The regional cybersecurity risk assessments shall identify, analyse, and evaluate the risks of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. The regional cybersecurity risk assessments shall not consider the legal, financial or reputational damage of cyber-attacks.

2. The regional cybersecurity risk assessments shall integrate the information from the cybersecurity risk assessments at Union level and at Member State level to provide a complete summary of the cybersecurity risks in the cross-border electricity cybersecurity risk assessment report.

Article 21 Regional cybersecurity risk treatment and acceptance

1. The ENTSO for Electricity in cooperation with the EU DSO entity and with the RCCs shall develop for each system operation region a cybersecurity risk treatment plan.

2. The regional cybersecurity risk treatment plans shall include:

   (a) the minimum and advanced security controls to be included in the common electricity cybersecurity framework pursuant to Article 23;

   (b) the measures the RCC shall apply in the system operation region;

   (c) the residual cybersecurity risks in the regions after applying the measures in paragraphs (a) and (b).

3. At least after every cybersecurity risk assessment cycle and whenever necessary the ENTSO for Electricity in cooperation with the EU DSO entity and with the RCCs shall update the risk treatment plans.

4. After every regional risk assessment, the ENTSO for Electricity and the EU DSO entity shall update the minimum and advanced cybersecurity requirements based on the regional cybersecurity risk treatment plans. The proposals for amendments shall be submitted to consultation and to opinion in accordance with the procedure set out in Article 5-8.

Article 22 Cross-border electricity cybersecurity risk assessment report

1. Within 15 months after the start of each risk assessment cycle, the ENTSO for Electricity and the EU DSO entity shall provide a report to assess cybersecurity risks with regard to cross-border electricity flows (the 'Cross-Border Electricity Cybersecurity Risk Assessment Report').

2. The report shall include at least the following information:

   (a) the list of Union-wide high-impact and critical-impact business processes identified in the Union-wide cybersecurity risk assessment including for each process the estimate of the possible risk of a cyber-attack on the process that was assumed during the regional cybersecurity risk assessment;

   (b) the inventory of the high level assets explicitly putting emphasis on:

      (i) legacy systems;

      (ii) assets that implement the highest level and lowest level of security;

      (iii) assets that contribute to the operation of the cross-border electricity flows.

   (c) current threats, with a specific focus on emerging threats and risks for the electricity system;

   (d) incidents for the previous period at Union level, providing a critical overview of how such incidents may have had an impact on electricity cross border flows;

   (e) overall status of implementation of the cybersecurity measures;

   (f) status of implementation of the critical information flows;

   (g) identified and highlighted risks that may derive from insufficient supply chain management;

   (h) results and accumulated experiences from mandatory regional and cross-regional cybersecurity exercises;

   (i) an analysis of the development of the overall cross-border cybersecurity risk in the electricity sector since the last regional cybersecurity risk assessment;

   (j) the regional cybersecurity risk treatment plansArticle 21;

   (k) any other information that may be useful to identify a partial failure of this Regulation or the need for a revision of this Regulation or any of its tools.

   All entities listed in Article 2(1) (a), (b), (c), (d), (e), (j), (k), (m) and (o) shall contribute to the development of the report, respecting the confidentiality of information in accordance with Article 10 and Article 11.

   The entities listed in Article 2(1) (h), (i), (l) and (n) may contribute to the development of the report. The ENTSO for Electricity and the EU DSO entity shall consult these entities from an early stage.

3. The report shall be subject to the rules on protection of exchange of information pursuant to Article 11.

4. Without prejudice to Article 10(3) a sanitised public version of the report may be released without the information that, for the nature of their confidentiality, may be released on "need-to-know basis" only. Before the release of the sanitised public version, the NIS Cooperation Group shall provide its approval of the sanitised public version of the report. The ENTSO for Electricity and the EU DSO entity are responsible for the compilation and the release of the sanitised public version of the

report.

TITLE IV
COMMON ELECTRICITY CYBERSECURITY FRAMEWORK

Article 23 Scope of the common electricity cybersecurity framework

1. The ENTSO for Electricity and the EU DSO entity shall jointly develop a proposal for a common electricity cybersecurity framework consisting of:

   (a) minimum cybersecurity controls that shall be applied by all high-impact and critical-impact entities inside the high-impact perimeter pursuant to Article 30;

   (b) advanced cybersecurity controls that shall be applied by all critical-impact entities inside the critical-impact perimeter pursuant to Article 30;

   (c) an electricity controls to standards mapping matrix ('ECSMM') that maps the controls from (a) and (b) to selected international standards and national legislative frameworks pursuant to Article 25.

2. The minimum and advanced cybersecurity controls shall include supply chain security controls in accordance with Article 24.

3. The minimum and advanced cybersecurity controls shall be verifiable by an accredited conformity assessment body in accordance with the procedure set out in Article 33.

Article 24 Minimum and advanced cybersecurity supply chain security controls

1. The ENTSO for Electricity and the EU DSO entity shall ensure that the minimum and advanced cybersecurity controls include minimum and advanced cybersecurity supply chain security controls that mitigate the supply chain risks identified in the regional cybersecurity risk assessment. The minimum and advanced cybersecurity supply chain security controls shall cover the entire lifecycle of all ICT products, ICT services and ICT processes inside the high-impact or critical-impact perimeters of an entity.

2. The minimum cybersecurity supply chain controls shall include controls for high-impact and critical-impact entities to:

   (a) include in the requirements for new ICT products, ICT services or ICT processes cybersecurity procurement requirements based on the results of the cybersecurity risk assessment at entity level. Entities may use the harmonized cybersecurity procurement requirements in accordance with Article 35. If entities define their own cybersecurity procurement requirements, these shall cover at least:

      (i) technical cybersecurity procurement requirements for the ICT product, ICT service or ICT process used, or to be used;

      (ii) background verification checks of the staff of the supplier involved in the supply chain and dealing with sensitive information or with access to the high-impact or critical-impact assets of the entity;

(iii) processes for secure and controlled design, development and production of ICT products, ICT services and ICT processes, promoting security-by-design and zero trust architectures;

(iv) controls over the access of the supplier to the assets of the entity;

(v) obligations of the supplier to protect sensitive information;

(vi) propagation of cybersecurity procurement requirements to subcontractors of the supplier to ensure that the cybersecurity procurement requirements apply throughout the supply chain;

(vii) traceability of the application of the cybersecurity procurement requirements from the development through production until delivery, maintenance and end of lifecycle of ICT products, ICT services or ICT processes;

(viii) support for security updates throughout the entire lifetime of ICT products, ICT services or ICT processes;

(ix) the right to audit design, development and production processes at the supplier.

(b) only select and contract suppliers that meet the cybersecurity procurement requirements as stated in paragraph (1) and that possess a cybersecurity level appropriate to the cybersecurity risk-level of the ICT product, ICT service, or ICT processes that the supplier delivers;

(c) diversify sources of supply for ICT products, ICT services and ICT processes and limit vendor lock-in;

(d) include the cybersecurity procurement requirements as stated (1) in contracts with suppliers, collaboration partners and other parties in the supply chain, covering ordinary deliveries of ICT products, ICT services and ICT processes as well as unsolicited events and circumstances like termination and transition of contracts in cases of negligence of the contractual partner;

(e) monitor, review or audit the cybersecurity procurement requirements for supplier processes throughout the entire lifecycle of each ICT service and ICT process on a regular basis.

3. The advanced cybersecurity supply chain security controls shall include controls for critical-impact entities to verify during procurement that ICT products, ICT services and ICT processes, that will be used as critical-impact assets, satisfy the cybersecurity procurement requirements. The ICT product, ICT service or ICT process shall either be verified through a verification scheme pursuant to Article 36 or shall be subject to verification activities. The depth and coverage of the verification shall be appropriate for the risks identified in the risk assessment at entity level. The critical-impact entity shall document the steps taken to reduce the risks identified.

Article 25 Electricity controls to standards mapping matrix

1. The ENTSO for Electricity and the EU DSO entity shall jointly map through the ECSMM the controls set out in Article 23 (1) (a) and (b) to selected international standards and shall track the conformity of the different controls with the controls set out in Article 23 (1) (a) and (b).

2. The CS-NCAs and NRAs may provide to the ENTSO for Electricity and the EU DSO entity a mapping of the controls set out in Article 23 (1) (a) and (b) of the national legislative frameworks. If the CS-NCA and NRA provide a mapping, they shall have a conformity assessment body verify

that the national requirements are sufficiently equivalent to the minimum and advanced cybersecurity controls. If the CS-NCA and NRA provide a mapping, the ENTSO for Electricity and the EU DSO shall integrate the national mappings into the ECSMM.

TITLE V
RISK ASSESSMENT AT MEMBER STATE LEVEL

Article 26 Member State cybersecurity risk assessment

1. Every cybersecurity risk assessment cycle each CS-NCA shall perform a cybersecurity risk assessment on all high-impact and critical-impact entities in its Member State using the methodology developed by the ENTSO for Electricity and the EU DSO entity in accordance with Article 17. The Member State cybersecurity risk assessment shall identify and analyse the risks of cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows. The Member State cybersecurity risk assessment shall not consider the legal, financial or reputational damage of cyber-attacks.
2. Within 9 months after the start of the cybersecurity risk assessment cycle each CS-NCA shall provide a Member State cybersecurity risk assessment report to the ENTSO for Electricity and the EU DSO entity, containing the following, information for each high-impact and critical-impact business process:
   (a) the overall likelihood and consequence on the risk impact matrix of a successful cyber-attack compromising the Union-wide high-impact and critical-impact business process in its Member State;
   (b) a summary of the threats and vulnerabilities that contribute to this likelihood;
   (c) the recommended controls to reduce this cybersecurity risk.

   The report shall also include a risk assessment of the temporary derogations issued by the NRAs and CS-NCAs in the Member States pursuant to Article 30.

   The ENTSO for Electricity and the EU DSO entity may request additional information from the CS NCAs in relation to the tasks specified in paragraph (2) (a), (b) and (c).
3. The CS-NCA shall ensure that the information they provide is accurate, correct, and not older than 6 months.

Article 27 Identification of high-impact and critical-impact entities

1. The CS-NCA shall identify the high-impact and critical-impact entities in its member state using the Union-wide impact assessment report. The CS-NCA may identify additional entities and their assets or processes as high impact or critical impact, even where they do not individually meet the ECII level, due to member state specific circumstances, having regard for the aggregated impact of multiple similar entities on cross border electricity flows.
2. In each risk assessment cycle, the CS-NCA shall within 6 months after receiving the Union-wide impact assessment report:
   (a) deliver to the ENTSO for Electricity and the EU DSO entity a list of high-impact and critical-

impact entities;

(b) notify the entities on the list that they have been identified as a high-impact or critical-impact entity.

Article 28 National verification schemes

1. The CS-NCA and the NRA may establish a national scheme to verify that critical-impact entities have implemented the national legislative framework that is included in the ECSMM. The national verification scheme may be based on inspection by the CS-NCA and / or the NRA, or on peer reviews by critical-impact entities in the same Member State supervised by the CS-NCA and / or the NRA.
2. If the CS-NCA and the NRA decide to establish a national verification scheme, the CS-NCA and the NRA shall ensure that the verification is performed according to the following requirements:
   (a) any party performing the peer review or inspection shall be independent from the critical-impact entity being verified, and shall have no conflicts of interest;
   (b) The staff performing the peer review or inspection shall have demonstrable knowledge of:
      (i) cybersecurity in the electricity sector;
      (ii) cybersecurity management systems;
      (iii) the principles of auditing;
      (iv) cybersecurity risk assessment;
      (v) the common electricity cybersecurity framework;
      (vi) the national legislative framework and international standards in scope of the verification;
      (vii) the critical-impact business processes in scope of the verification.
   (c) The party performing the peer review or inspection shall be allowed sufficient time to perform these activities. The time allowed for the activities shall be comparable to the time required for the certification of the cybersecurity management system with comparable scope by a conformity assessment body. The calculation of overall peer review or inspection time shall include sufficient time for reporting.
   (d) The party performing the peer review, or inspection shall take sufficient measures to protect the confidential information they collect during the verification.
3. If the CS-NCA and the NRA decide to establish a national verification scheme, the CS-NCA and the NRA shall report on an annual basis the frequency of inspections performed under the national verification scheme to ACER.

TITLE VI
RISK MANAGEMENT AT ENTITY LEVEL

Article 29 Cybersecurity risk management at entity-level

1. Each high-impact and critical-impact entity as identified by the CS-NCA shall perform a cybersecurity risk management for all its assets in its high-impact and critical-impact perimeters. Each high-impact and critical-impact entity shall perform a risk management cycle covering the phases in (2) at least every two years.
2. Each high-impact and critical-impact entity shall use a cybersecurity risk management approach that applies the following phases:
   (a) context establishment;
   (b) cybersecurity risk assessment;
   (c) risk treatment;
   (d) risk acceptance;
3. During the context establishment phase, each high-impact and critical-impact entity shall:
   (a) define the scope of the cybersecurity risk assessment including at least the high-impact and critical-impact processes identified by the ENTSO for Electricity and the EU DSO entity;
   (b) define criteria for risk evaluation and for risk acceptance in line with the risk impact matrix defined by the ENTSO for Electricity and the EU DSO entity.
4. During the cybersecurity risk assessment phase, each high-impact and critical-impact entity shall:
   (a) identify risks by taking into account:
      (i) all assets supporting the Union-wide high-impact and critical-impact processes, including all supply chain processes with an assessment of the possible impact on cross-border electricity flows if the asset is compromised;
      (ii) possible threats taking into account the threats identified in the latest Cross-Border Electricity Cybersecurity Risk Assessment Report and supply chain threats;
      (iii) vulnerabilities including those caused by legacy systems;
      (iv) possible cybersecurity incident scenarios, including cyber-attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows;
      (v) existing implemented controls.
   (b) analyse the likelihood and consequences of the cybersecurity risks identified in (a) and determine the cybersecurity risk level using the risk impact matrix.;
   (c) classify assets according to the possible consequences of a compromise and determine the high-impact and critical-impact perimeter using the methodology defined by the ENTSO for Electricity and the EU DSO entity;
   (d) evaluate risks by prioritizing the cybersecurity risks against risk evaluation criteria and risk acceptance criteria as defined in paragraph (3)(b).

5. During the risk treatment phase, each high-impact and critical-impact entity shall establish a risk treatment plan by selecting risk treatment options appropriate to manage the risks and identify the residual risks after treatment. Each entity shall report the controls it implements for risk treatment to its NRA and its CS-NCA.

6. During the risk acceptance phase, each high-impact and critical-impact entity shall decide whether to accept the residual risk based on the risk acceptance criteria established in paragraph (3)(b).

7. Each high-impact and critical-impact entity shall register the assets identified in paragraph (2) in an asset inventory that includes all interfaces with the environment in which the entity operates.

Article 30 Derogations from the minimum and advanced cybersecurity controls

1. Within 6 months after the finalisation of the minimum and advanced cybersecurity controls, all entities listed in Article 2 (1) shall during the risk treatment step pursuant to Article 29 apply the minimum cybersecurity controls within the high-risk perimeter and advanced cybersecurity controls within the critical impact perimeter.

2. The NRAs and the CS-NCAs may jointly provide derogations for any entity listed in Article 2 (1) seated in their Member State from the minimum and advanced cybersecurity controls in one of the following cases:

   (a) in exceptional circumstances, when the entity can demonstrate that the costs of implementing the appropriate cybersecurity controls significantly exceed the benefit;

   (b) The entity can provide a risk treatment plan that mitigates the cybersecurity risks using alternative controls to a level that is acceptable according to the risk acceptance criteria pursuant to Article 29(3)(b). The risk treatment plan shall be verified through one of the options pursuant to Article 33.

   (c) The results of the risk assessment of the entity do not show any direct or indirect impact on cross-border electricity flows.

3. Derogations from the minimum or advanced cybersecurity controls shall be granted for a maximum of two years. Before granting the derogation the NRAs and the CS-NCAs shall consult the entities that are affected by the derogation.

4. The list of the derogations shall be included as an annex to the Cross Border Electricity Cybersecurity Risk Assessment Report. The ENTSO for Electricity and the EU DSO entity shall jointly update the list when necessary.

Article 31 Reporting on the risk assessment at entity level

1. Each high-impact and critical-impact entity shall within 6 months after the start of each cybersecurity risk assessment cycle provide to the CS-NCA the following information for the Member State cybersecurity risk assessment:

   (a) a summary of threats, existing controls, and vulnerabilities;

   (b) an estimate of the consequences and likelihood of a compromise of the confidentiality, integrity, and availability of the Union-wide high-impact and critical-impact processes that they are involved in mapped to the risk impact matrix;

The CS NCA may request additional information from the high impact and critical impact entity.

2. The entity shall ensure that the information they provide is accurate, correct, and not older than 6 months.

Article 32 Cybersecurity management system

1. Within 12 months after being notified by the CS-NCA and NRA in accordance with Article 27, all high-impact and critical-impact entities shall establish a cybersecurity management system that is based on an international standard and that meets the requires entities to:

   (a) determine the impact upon the parties affected by the security risks for each asset of the entity and the scope of the management system considering interfaces and dependencies with other entities;

   (b) demonstrate leadership and commitment of top management with respect to the management system;

   (c) ensure that the resources needed for the management system are available;

   (d) establish a cybersecurity policy that shall be documented and communicated within the entity and to parties affected by the security risks;

   (e) assign and communicate responsibilities for roles relevant to cybersecurity;

   (f) perform cybersecurity risk management as defined in Article 29;

   (g) determine and provide the resources required for implementation, maintenance and continual improvement of the management system; these shall consider the determination of the necessary competence and awareness of cybersecurity resources;

   (h) determine the need for internal and external communications relevant to cybersecurity;

   (i) create, update and control documented information related to the management system;

   (j) evaluate the cybersecurity performance and effectiveness of the cybersecurity management system;

   (k) conduct internal audits at planned intervals to ensure that the management system is effectively implemented and maintained;

   (l) obligations for top management to review the implementation of management system at planned intervals;

   (m) control and correct non-conformity to the management system.

2. The scope of the cybersecurity management system shall include all assets within the high-impact and critical-impact perimeter of an entity.

Article 33 Verification of the common electricity cybersecurity framework

1. No later than 24 months after publication of the common electricity cybersecurity framework each critical-impact entity shall demonstrate its compliance with the management system and the minimum or advanced cybersecurity controls that are part of the common electricity cybersecurity framework.

2. The entity shall verify compliance by one of the following options:

   (a) being certified or audited by an independent conformity assessment body;

   (b) being verified by a national verification scheme.

3. The verification of compliance shall cover all assets within the critical-impact perimeter.

Article 34 Cybersecurity inspections

When exercising their supervisory task over critical impact and high impact entities, the CS-NCAs shall have the powers to:

(a) carry out on-site individual and coordinated multi-site joint inspections,

(b) carry out off-site supervision, including random checks;

(c) make random inspections to verify the implementation of the cybersecurity management system and the compliance with the minimum or advanced cybersecurity controls;

(d) request the information necessary to assess the cybersecurity measures, including the results of the risk assessment at entity level, cybersecurity policies and audit reports.

TITLE VII
HARMONISED CYBERSECURITY PROCUREMENT REQUIREMENTS

Article 35 Harmonising cybersecurity procurement requirements

1. The ENTSO for Electricity and the EU DSO entity shall set up a rolling work programme to develop harmonised cybersecurity procurement requirement sets that for high-impact and critical-impact entities may use as a basis for the procurement of ICT products, ICT services and ICT processes in the high-impact and critical-impact perimeters. The ENTSO for Electricity and the EU DSO entity shall develop:

   (a) a reference architecture to describe and classify the types of ICT products, ICT services and ICT processes used by high-impact and critical-impact entities in the high-impact and critical-impact perimeter;

   (b) harmonised cybersecurity procurement requirement sets for ICT products, ICT services and ICT processes from the reference architecture that entities can use in their procurement processes.

   The ENTSO for Electricity in cooperation with the EU DSO entity shall select the types of ICT products, ICT services, and ICT processes for which harmonised cybersecurity procurement requirement sets are developed based on the priorities of high-impact and critical-impact entities.

The harmonised cybersecurity requirement sets shall be based on the outcomes of the cybersecurity risk assessment at regional level.

The ENTSO for Electricity and the EU DSO entity shall ensure that the set of cybersecurity procurement requirement is compatible with Union certification schemes. In particular, they shall ensure that the applicable security objectives in Article 51 of Regulation (EU) 2019/881 are met by

the ICT products, ICT services and ICT processes.

2. The ENTSO for Electricity and the EU DSO entity shall publicly consult the proposal for the harmonised cybersecurity procurement requirements. The consultation shall last at least one month. The ENTSO for Electricity and the EU DSO entity shall take into account the views provided by all involved entities.

3. The ENTSO for Electricity and the EU DSO entity shall update the harmonised cybersecurity procurement requirements, when necessary. The proposals for amendments shall be submitted to consultation and to opinion in accordance with the procedure set out in paragraph (2).

Article 36 Union verification schemes for ICT products, ICT services and ICT processes

1. The ENTSO for Electricity and the EU DSO entity may develop guidance on the Union verification schemes that help critical-impact entities to determine whether an ICT product, ICT service or ICT process meets the harmonised cybersecurity procurement requirements.

2. Without prejudice to the framework for the establishment of European cybersecurity certification schemes pursuant to Article 46 of Regulation (EU) 2019/881, the ENTSO for Electricity and the EU DSO entity may provide sector-specific guidance on the use of European cybersecurity certification schemes, whenever a suitable scheme is available for a type of ICT product, ICT service or ICT process. This sector-specific guidance may include additional testing requirements and rules for classifying vulnerabilities. If a suitable European certification scheme is not available, the ENTSO for Electricity and the EU DSO entity may develop sector-specific guidance on the application of an existing European cybersecurity certification scheme for a certain type of ICT product, ICT service or ICT process.

3. The ENTSO for Electricity and the EU DSO entity shall closely cooperate with ENISA when developing the guidance in accordance with paragraphs (1) and (2). The ENTSO for Electricity and the EU DSO entity shall consult the main stakeholders on the guidance in accordance with Article 8. The ENTSO for Electricity and the EU DSO entity shall take into account the views provided by all involved entities before finalising the guidance.

TITLE VIII
ESSENTIAL INFORMATION FLOWS, INCIDENT AND CRISIS MANAGEMENT

Article 37 Role of CSIRTs in case of a cyber-incident or cyber attack

1. The CS-NCA or CSIRT pursuant to Articles 8 and 9 of Directive (EU) 2016/1148 shall be responsible for the collection, the sanitisation, the properly anonymization and the dissemination of data in case of a cyber-incident or cyber-attack.

2. CSIRTs shall have the right to share capabilities with other CSIRTs in other Member States following an agreement among the concerned CSIRTs.

3. CSIRTs may delegate fully or partly its responsibilities concerning one or more specific electricity entities that operates in more than one Member State, to another CSIRT. Before delegating such a responsibility the CSIRT, the concerned entity and the CSIRT of the other Member State shall

conclude an agreement to determine how and when, the delegating CSIRT shall be kept informed by the other CSIRT during the delegation period.

4. In the event of a cyber-incident or cyber-attack, the CS-NCA or the CSIRT shall assess the level of classification of the information received from the entity and shall inform the entity about the outcome of its assessment within eighteen (18) hours of receipt of the information. The CS-NCA or the CSIRT shall not disseminate information and withhold it as long as the information constitutes a high risk and could harm, hinder or disrupt the investigation of an ongoing cyber-attack.

   The CSIRT shall be responsible for proactively verifying and finding any other similar incident in the Union reported to other CSIRTs, to correlate information provided in the context of the incident from other incidents in order to eventually enrich existing information, strengthen and coordinate cybersecurity responses.

5. The CSIRT shall:

   (a) share information with the CSIRT network within eighteen (18) hours after the reception of a reportable cyber security incident and provide updated information on a regular basis to the CSIRTs until the incident is closed;

   (b) disseminate reportable cybersecurity incident information received from the CSIRT network to critical impact and high impact entities in its Member State within in two (2) hours after the determination of relevant technical information allowing the entities to organize effectively their cybersecurity defence;

   (c) disseminate to the CSIRT network and to the entities in its Member State within twenty-four (24) hours information on cyber threats or any other information of importance for preventing, detecting, responding to or mitigating the risk;

   (d) not share vulnerabilities such as 0 day vulnerabilities not publicly known as long as the vendor does not provide the patch or other mitigation measures to the concerned entity;

   (e) support, in cooperation with ENISA the concerned entity to receive from the vendor an effective and rapid management of the 0 day vulnerability;

6. ENISA shall provide the entities with non-binding guidance on establishing CSOC capabilities or engaging with MSSPs.

7. The ENTSO for Electricity with the support of the EU DSO Entity and with the support of ENISA, shall develop a cyber-security incidents classification scale methodology within twelve (12) months after the entry into force of this Regulation.

   The methodology shall:

   (a) provide the classification for the gravity of an incident according to 5 levels, the two highest level being “High” & “Critical”;

   (b) the classification shall be based on the assessment of the following parameters:

      (i) the criticality of the asset exposed that will be determined during the asset inventory and its proximity to other more critical assets;

      (ii) the severity, the depth and the surface of the cyber-attack.

8. Within two (2) years after entry into force of this Regulation, the ENTSO for Electricity and the

EU DSO entity shall assess the possibility and the financial feasibility to develop a common tool for all entities with automatic connections to the CSIRT network tools.

The feasibility study that shall take into account the following:

(a) such a tool shall support critical impact and high impact entities with relevant security related information for operations of cross border electricity flows, such as near real-time reporting of cybersecurity incidents, early warnings related to cybersecurity matters and undisclosed vulnerabilities on equipment in use in the electricity system;

(b) such a tool shall be maintained through a suitable and highly trustable environment. National and international information sharing networks shall be protected using state of the art best practice techniques and standards;

(c) such a tool shall allow for data collection from critical impact and high impact entities and facilitate sanitisation and anonymisation of the data and its prompt dissemination to critical impact and high impact entities.

The ENTSO for Electricity and the EU DSO entity shall analyse and facilitate initiatives proposed by electricity entities to test such tools.

The ENTSO-E for Electricity and the EU DSO entity shall consult ENISA, the CSIRT network and the representatives of main stakeholders when assessing the feasibility.

The ENSO-E for Electricity and the EU DSO entity shall present the results of the feasibility study to ACER.

Article 38 Data collection, sanitisation and dissemination

1. Each high-impact and critical impact entity shall:

   (a) establish at least the following CSOC capabilities:

      (i) ensure that relevant systems and applications provide security logs for security monitoring to enable the detection of anomalies and collect information on security incidents;

      (ii) conduct security monitoring including but not limited to the intrusion the detection and the vulnerability scanning of network and information systems within the cybersecurity perimeter of the entity pursuant to Article 29 (4)(c);

      (iii) analyse and, if necessary, take all actions required under its responsibility and capacity to protect the entity;

      (iv) participating in the information collection and sharing described in this Article.

   (b) encourage the provision of automated tools including artificial intelligence for the capabilities described in paragraph 1(a);

   (c) without prejudice to paragraph 1(a), have the right to procure all or parts of the CSOC capabilities pursuant to paragraph 1(a) through MSSP or another entity providing the service;

   (d) designate a single point of contact for the purpose of information sharing with any external entity.

2. Each critical impact entity and each high impact entity shall share any information related to a

reportable cybersecurity incident with its CS-NCA or its CSIRT not later than four (4) hours after its determination.

A cybersecurity incident shall be considered reportable when all the parameters concerning the incident:

(a) are assessed and confirmed by the authorised representative of the entity;

(b) lead to the determination of a cybersecurity incident ranging from "high"' to "critical" following the cybersecurity incident classification scale methodology pursuant to Article 37 (7).

3. Each critical impact entity and each high impact entity shall share any information related to 0 day vulnerabilities not publicly known to CS NCA or CSIRT at national level, not later than twenty-four (24) hours after its determination by the CS NCA.

4. Each critical impact entity and each high impact entity shall share any information related to a cyber-threat if the following cybersecurity information is collected in the entity's own environment or in the environment of its service provider.

A cyber-threat information shall be considered reportable when:

(a) it is a near miss;

(b) the attack connected to third parties with which the entity has a commercial or a work-related relationship;

(c) the identified artifacts used in the context of the attack such as indicators of compromise, compromised URL or IP addresses, hashes or other attributes of malware;

(d) there are identified indicators of attacks;

(e) other information of importance for preventing, detecting, responding or mitigating impact or risk concerning cybersecurity risks.

5. Without prejudice to the reporting obligations under Directive (EU) 2016/1148, each critical impact entity and high impact entity shall – when reporting information pursuant to this Article – also stipulate:

(a) the legal basis under which the information is reported, including references to this Regulation;

(b) the kind of information shared: reportable cybersecurity incident, 0 days vulnerabilities not publicly known or threat;

(c) in the case of a reportable cybersecurity incident, the level of the incident according to the cybersecurity ICS methodology and all information leading to this classification including at least the criticality of the incident.

6. Each critical impact entity and high impact entity shall alert the CS NCA or the CSIRT in its Member State by clearly identifying specific information that shall only be with the CS NCA or the CSRIT in cases where the information sharing could cause harm. Entities shall have the right to provide a sanitised version of the information to the CSIRT.

Article 39 Detection of incidents and handling of incident related information

1. Critical impact and high impact entities shall develop the necessary capabilities to manage detected cyber incidents with the necessary support from the CS NCA, CSIRTs, the CSIRT network, the ENTSO for Electricity, the EU DSO entity, the RCCs and ENISA.

2. Critical impact and high impact entities shall implement effective processes to identify, classify and respond to cybersecurity incidents that will or may affect cross-border electricity flows in order to minimize the impact of a cyber-incident and cyber-attack and to react rapidly.

3. In case of incident has a cross-border effect, affected critical impact and high impact entities. CSOCs or MSSPs shall joint their effort to share information coordinated by the CS NCA or the CSIRT of the Member State in which the incident was reported the first time.

4. For coordination CSIRT Network standard operating procedure shall be used.

5. Critical impact and high impact entities shall:

   (a) report reportable cybersecurity incidents pursuant to Article 38 (2);

   (b) ensure that their own CSOC or MSSP have access to the information provided by the CSIRT network through their CSIRT at a need-to-know level;

   (c) establish incident management procedures for cybersecurity incidents, including roles and responsibilities, tasks and reactions based on the observable evolution of the incident within the critical impact and high impact entity and in the nearby cybersecurity perimeters;

   (d) Test incident response procedures at least every year. These test also can be conducted by critical risk and high impact electricity entities during the regular exercises according to article 43. Any live incident response activities (including lessons learnt) with a consequence classified at least Scale 3 according to the incident classification scale methodology, can serve as an annual test of the incident response plan;

   (e) provide specific requirements to handle incidents with potential cross-border effects, based on the principle of proximity to the incident.

Article 40 Crisis management

1. The critical impact or high impact entity impacted by a cross-border electricity crisis shall investigate in cooperation with its CS NCA or its CSIRT the root cause of the incident to determine whether the crisis is caused by a cybersecurity incident.

2. When a cybersecurity cross-border electricity crisis is declared by the CS NCA, the CS NCA or the CSIRTs from the affected Member States shall jointly create an ad hoc cybersecurity coordination group. The cybersecurity ad hoc coordination group shall:

   (a) provide relevant cybersecurity information to the electricity entities involved in the crisis management process;

   (b) coordinate cybersecurity measures to remediate the cybersecurity cross-border crisis;

   (c) provide the expertise required to the entities impacted by the cybersecurity cross-border crisis.

3. Critical impact and high impact entities covered by this Network Code shall liaise the Crisis Liaison Organisation Network (CyCLONe) through their national or sectorial representatives. The ad-hoc cybersecurity coordination group shall have the authority to take part in the CyCLONe.

4. On a Member State level, CS NCA or CSIRTs shall define the participants in the crisis management process such as electricity entities.

5. Critical impact and high impact entities shall develop and have available capabilities, internal guidelines, preparedness plans, and staff to take part in the detection and mitigation of cybersecurity cross-border crisis, with the support of its CS NCA, NRA, CSIRTs, the CSIRT Network, ENISA and RCCs, shall provide the necessary support to these entities in order to actively manage the crisis.

6. Each CS NCA or CSIRTs shall:

   (a) report the cybersecurity cross-border crisis to Europol and to national police;

   (b) inform the European External Action Service in case the cybersecurity cross-border crisis entails an important external policy dimension.

Article 41 Crisis management plans and business continuity

1. ACER shall develop a Union-level cybersecurity crisis management plan for the electricity sector. ACER shall closely cooperate with ENISA, with the ENTSO for Electricity, the EU DSO entity, and the NRAs when developing the plan.

2. Each NRA shall develop a national cybersecurity crisis management plan for the electricity sector taking into account the Union-wide cybersecurity crisis management plan developed by ACER. The NRA shall coordinate with the critical impact and high impact entities, the CS-NCA and RP-NCA in its Member State.

3. Critical impact and high impact electricity entities shall assure that:

   (a) cross border cybersecurity incident handling procedures are incorporated in their crisis management plans;

   (b) their cybersecurity-related crisis management processes are part of the general crisis management activities and compatible with incident handling processes.

4. Critical impact and high impact entities shall develop a crisis management plan for a cybersecurity-related crisis which is incorporated into their general crisis management plans and which shall include at least the following:

   (a) rules of declaration of the crisis as described in Article 14 (2) and (3) of the Regulation (EU) 2019/941;

   (b) clear roles and responsibilities for crisis management, including the role of other relevant critical impact and high impact electricity entities;

   (c) up-to-date contact information as well as rules for communication and information sharing during a crisis situation including the connection to the CSIRT.

   The crisis management plans have to be tested during the cybersecurity exercises as described in Article 43 and 44 of this Regulation.

5. The critical impact and high impact entities shall incorporate their crisis management plans into their business continuity plans for the critical processes. The crisis management plans at entity level shall include:

   (a) processes depend on availability, integrity and reliability of IT services;

(b) all business continuity locations including the locations for hardware and software;

(c) all internal roles and responsibilities connected to business continuity processes.

The critical impact and high impact entities shall update their crisis management plans at least every three years and whenever necessary.

6. The critical impact and high impact entities shall test their business continuity plans at least once every 3 years or after major changes in a critical business process. The outcome of the business continuity plan tests shall be documented. The critical impact and high impact entities may include the test of their business continuity plan in the cybersecurity exercises.

   In case a test identifies deficiencies in the business continuity plan, the critical impact and high impact entity shall correct those deficiencies within 180 calendar days after the testing and shall conduct a new test to provide evidence that the corrective measures are effective.

   In case a critical impact or high impact entity cannot correct the deficiencies within 180 calendar days, it shall report to its NRA according to Article 31.

   The critical impact and high impact entities shall update their business continuity plan whenever necessary and at least once every 3 years taking into account the outcome of the test.

Article 42 Cybersecurity early warning capabilities for the electricity sector

1. ENISA shall facilitate the Electricity Cybersecurity Early Warning Capabilities (ECEWC). ENISA shall ensure the ECEWC is operable within 3 years after the entry into force of this Regulation. ENISA shall cooperate closely with NCAs and relevant research institutions.

2. ENISA shall:

   (a) collect voluntary shared information from:

      (i) CERT-EU, CSIRTs network, CyCLONe, CSIRTs;

      (ii) the entities listed in Article 2 (1);

      (iii) any other entities to share voluntarily relevant information.

   (b) assess and classify collected information according to Traffic Light Protocol (TLP);

   (c) scan the information ENISA has access to for identifying cyber risk conditions and relevant indicators for aspects of cross-border electricity flows;

   (d) identify conditions and indicators that frequently correlate with larger cyber-attacks within the electricity sector;

   (e) define whether further analysis and preventive actions shall be taken through assessment and identification of risk factors;

   (f) inform the competent authorities or the CSIRTs on the identified risks and recommended preventive actions specific to the entities concerned;

   (g) inform all entities listed in Article 2 on the result information assessed on paragraph 2(b), (c) and (d);

   (h) periodically develop a situational awareness report.

3. The CSIRTs shall disseminate the information received from ENISA to the entities without undue delay from receipt.

4. The ENTSO for Electricity with the assistance of EU DSO Entity shall monitor the effectiveness of ECEWC. The analysis shall be part of the reporting pursuant to Article 12.

TITLE IX
ELECTRICITY CYBERSECURITY EXERCISE FRAMEWORK

Article 43 Cybersecurity exercises at entity and Member State level

1. In [year of publication +3] and every three years afterwards, each critical impact entity shall organise and perform a cybersecurity exercise at entity level including one or more scenarios with incidents affecting directly or indirectly cross-border electricity flows.

2. By derogation from paragraph 1, the NRA after consultation with CS-NCA, RP-NCA may request all critical impact entities of its Member State to participate in a cybersecurity exercise at national level instead of performing the cybersecurity exercise at entity level.

   If the NRA decides to organise a cybersecurity exercise at national level, the NRA shall send to the critical impact entities of its Member State the request that they shall participate in the cyber security exercise at national level at the latest by 30 June of the year preceding the cybersecurity exercise at entity level and at least 6 months before the cybersecurity exercise at national level takes place.

   The NRA may propose to incorporate this electricity cybersecurity national exercise into a national cybersecurity exercise. In order to be able to join the national cybersecurity exercise, NRA may deviate from the usual exercise rhythm for up to one year concerning national cybersecurity exercise.

3. The NCA shall organise the cybersecurity exercise at national level.

   In [year following the publication] and every three years afterwards, the ENTSO for Electricity in cooperation with the EU DSO entity, shall make available an exercise scenario template, built on the most recent risk assessment results performed, for each of the exercises referred to in paragraph 1. The ENTSO for Electricity in cooperation with the EU DSO entity shall consult ACER and ENISA on the template.

Article 44 Regional or cross regional cybersecurity exercises

1. In [year of publication +4] and every three years afterwards, in each system operation region, the ENTSO for Electricity in cooperation with the EU DSO entity and the concerned RCC shall organise a cybersecurity exercise. The critical impact entities in the system operation region shall participate in the cybersecurity exercise. The ENTSO for Electricity may decide to organise cross regional cybersecurity exercises instead of one exercise per system operation region.

2. ENISA shall support the ENTSO for Electricity and the EU DSO Entity in the preparation and organisation of the cybersecurity exercise at regional or at cross-regional level.

3. The ENTSO for Electricity in coordination with EU DSO shall inform 6 months before the exercise takes place the entities that shall participate in the exercise.

4. If Cyber Europe exercise or any mandatory cybersecurity exercise relate to energy sector within the same geographic perimeter, by derogation from paragraph 1, the organizer of such exercise shall invite the ENTSO for Electricity and EU DSO entity to participate.
   In order to be able to join the Cyber Europe Exercise, the ENTSO for Electricity in coordination

with EU DSO entity may deviate from the usual exercise rhythm for up to one year concerning regional or cross regional cybersecurity exercise.

5. In [second year following the publication] and every three years, the ENTSO for Electricity with the support of EU DSO entity shall make available an exercise template, built on the major risks identified as a result of the top-down risk assessment performed in accordance with Article 21. The ENTSO for Electricity shall consult the Commission and may seek advice of ACER, ENISA and the Joint Research Centre.

Article 45 Internal, national, regional or cross-regional cybersecurity exercises

1. The critical impact entities shall require their critical service providers providing services in the area corresponding with the scope of the exercise, to participate in the exercise referred in Article 43 (1), Article 43 (2) and Article 44 (1). The critical impact entities shall include in their contract with their suppliers the obligation to participate in the cybersecurity exercise.

2. Depending on the size, the scenario and the expected outcome, the cybersecurity exercises organizers shall alternate the types of cybersecurity exercises.

3. The cybersecurity exercises organizers, with the advice of ENISA if requested by the organizer, shall analyse and finalize the exercise through a lesson-learnt report at destination to all participants including at least the exercise scenario, meeting reports, main positions and lessons learnt at any level of the electricity value chain. Lessons learnt shall focus on improvement of tasks to correct, adapt or change cybersecurity crisis processes, associated governance models, and, potentially, contractual engagements with critical service providers. The entities participating in the exercise shall participate in the tasks and implement the actions agreed .

4. For the follow-up of the internal and national exercises, organizers defined in Article 43(1) and Article 43(2) shall consult participants and follow a periodic analysis of the implementation of the lessons learnt and recommendations.

5. For the follow-up of the regional exercises or cross-regional exercises defined in Article 44, the ENTSO for Electricity and the EU DSO entity shall consult the critical impact entities and other participants in the exercise and include a periodic analysis of the lessons learnt and recommendations.

TITLE X
PROTECTION OF INFORMATION EXCHANGED IN THE CONTEXT OF THIS DATA PROCESSING

Article 46 Basic principles and minimum standards

1. All information exchanged between and handled internally by the entities defined in Article 2 for the implementation of this Regulation shall be protected according to the rules of TITLE X, considering the level of classification of the information applied to the information by the originator. Any provisions on confidentiality and protection of data in this Regulation shall be without prejudice to existing legislation for the protection of commercially sensitive, confidential information and trade secrets, and in particular, consistent with Regulation (EU) 2016/679 and Regulation (EU) 1227/2011.

2. Protection of information, regardless of its form, shall balance transparency, proportionality, accountability and efficiency with the need to protect information from unauthorised access, use, disclosure, modification or destruction.

3. Protection of information shall be aimed at protecting confidentiality, integrity and availability.

4. Risk management processes shall therefore be used to classify information assets and to develop proportionate security measures, procedures and standards, including mitigating measures.

5. When deemed necessary for the protection of confidentiality, the entity providing or sending information required by this Regulation shall classify the confidential information either as:

   (a) 'European Union Classified Information' (hereafter 'EUCI') or the applicable equivalent national classification, that is to say any information or material designated by an EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States, as stated in Commission Decision (EU, Euratom) 2015/444;

   (b) 'Sensitive non-classified information', that is to say information or material the entities defined in Article 2 must protect because of legal obligations laid down in the Treaties or in acts adopted in implementation thereof, and/or because of its sensitivity. Sensitive non-classified information includes, but is not limited to, information or material covered by the obligation of professional secrecy, as stated in Art 6 of this Regulation, (as referred to in Article 339 TFEU, information covered by the interests protected in Article 4 of Regulation (EC) No 1049/2001 read in conjunction with the relevant case-law of the Court of Justice of the European Union or personal data within the scope of Regulation (EU) 2016/679) and sensitive information regulated by applicable Member State regulations for the energy sector or critical infrastructure.

6. The entity providing or sending information that do not need protection of confidentiality according to paragraph 5, shall classify the information as NCCS Unrestricted.

7. When multiple sets of information are aggregated into a single set, the applicable level of classification is equal to the highest level of confidential information classification among the original sets. The rank of confidential information classifications levels defined by this Regulation shall be:

   (a) EU Classified Information as defined in paragraph 5(a)

   (b) Sensitive Non-Classified Information as defined in paragraph 5(b)

   (c) NCCS Unrestricted as defined in paragraph 6.

Article 47 Rules for Marking and Protection of Confidential Information

1. All entities entity sending information required by this Regulation shall mark the confidential information in line with the classification according to Article 38 (2), (3) and (4) either as EU Classified Information (EUCI or the applicable equivalent national classification), Sensitive Non-classified Information according to relevant national and Union regulations or NCCS Unrestricted.

   In addition to the classification marking, the sending entity shall mark the classified information with an identifier of the classifying organisation, and optionally additional markings to designate field of activity to which it relates, limit distribution, restrict use or indicate releasability.

2. For information shared in the context of Chapter VIII the information classified as Sensitive Non-

classified Information or NCCS Unrestricted the sending entity shall additionally mark the information according to the informal Traffic Light Protocol (TLP label)[1] to indicate distribution limitation. TLP labels 'TLP:RED', 'TLP:AMBER' and 'TLP:GREEN' shall only be applicable for information classified as Sensitive Non-classified Information. The TLP label 'TLP:WHITE' shall only be applicable for information classified as NCCS Unrestricted.

3. Information not marked with mandatory classification marking, identifier of the classifying organisation or TLP label by the entity sending information according to paragraph (1) shall be handled by the receiving entities as non-conformant to the protection rules of this regulation and be refused by the receiving entity. The receiving entity shall inform the NRA (or CS-NCA) in case of reception of non-conformant information.

4. Information marked as EU Classified Information (EUCI) or the applicable equivalent national classification shall be handled and protected by the receiving entities according to the rules stated in Commission Decision (EU, Euratom) 2015/444.

5. Information marked as Sensitive Non-classified Information shall be subject to entity internal rules regarding its internal handling, storage and dissemination respecting the classification marks and TLP labels. It shall only be released to those individuals who have a 'need-to-know'. When deemed necessary for the effective protection of its confidentiality, it shall be identified by a marking as Sensitive Non-classified Information (or equivalent) and corresponding secure handling instructions approved by management of the entity. When handled or stored on communication and information systems, such information shall be protected according to this Regulation and other applicable Union and Member State legislation, its implementing rules and corresponding best practice standards.

6. Information to be published shall be restricted to information classified as NCCS Unrestricted only.

7. Information received with a TLP label shall only be shared internally and externally in accordance with the Traffic Light Protocol[2]. If there is a need to share the information more widely than indicated by the original TLP label designation, recipients must obtain explicit permission from the original source.

Article 48 Protection of information exchanged in the context of Title VIII

1. Each entity listed in Article 2 sending information in the context of Title VIII, shall prior to sending

   (a) classify the information according to Article 46 considering all regulations, including Regulation (EU) 2016/679, Regulation (EU) 1227/2011, protection of national defence secrets, the regimes for the protection of commercially sensitive and confidential information and regime for the protection of trade secrets; and

   (b) determine the distribution restrictions according to the Traffic Light Protocol3 in accordance with Article 47 (2); and

   (c) ensure that ownership is stated identifying the classifying organisation and the source of information.

[1] Traffic Light Protocol (TLP) — Version 1.0 https://www.first.org/tlp

[2] Traffic Light Protocol (TLP) — Version 1.0 https://www.first.org/tlp

[3] Traffic Light Protocol (TLP) — Version 1.0 https://www.first.org/tlp

2. Each entity listed in Article 2 receiving information in the context of Title VIII, shall:

   (a) have the responsibility to protect the information according to the confidentiality classification marking;

   (b) distribute information internally and externally according to the TLP label restriction as part of the necessary information processing and following the "need to know" principle.

3. A competent authority or a CSIRT receiving information the context of Chapter VIII, shall, when needed for sharing the information more widely than indicated by the original TLP label designation, be entitled to:

   (a) modify, change or adapt the information received in order to anonymize and sanitize the information and avoid any harm to the entity sharing the information; in order to

   (b) relabel the information provided that an explicit permission is obtained from the original source of information.

4. If for the purpose of paragraph (3) above, a reclassification of classified information is relevant, the classification of the modified classified information shall be done by the competent authority or CSIRT after consultation and approval of the default classifying organisation.

TITLE XI
FINAL PROVISIONS

Article 49 Transitional provisions

1. Within 2 months after entry into force of this Regulation, the ENTSO for Electricity and the EU DSO entity shall develop a transitional electricity cybersecurity impact index. The ENTSO for Electricity and the EU DSO entity shall notify the transitional electricity cybersecurity impact index to the CS-NCAs and the NRAs.

2. Within 2 months of receipt of the transitional electricity cybersecurity impact index the CS-NCAs and the NRAs shall identify high-impact and critical-impact entities in their Member State based on the transitional electricity cybersecurity impact index and shall develop a transitional list of high impact and critical impact entities. The transitional list of high impact and critical impact entities shall be based on a precautionary principle, so that entities may only gain more responsibilities in the revised list after the end of the transition period, compared to where they stand in the national transitional list of high-impact and critical-impact entities. The CS-NCAs and the NRAs shall notify to the ENTSO for Electricity and the EU DSO entity their transitional list of high-impact and critical-impact entities.

3. Within 6 months after entry into force of this Regulation the ENTSO for Electricity in cooperation with the EU DSO entity shall consolidate the national transitional lists of high impact and critical impact entities received from the CS-NCAs and the NRAs. The ENTSO for Electricity in cooperation with the EU DSO entity shall consult ACER, the Commission, ENISA, the CS-NCAs and the NRAs on the consolidated transitional list of high impact and critical impact entities. The ENTSO for Electricity in cooperation with the EU DSO entity shall amend the proposal, if necessary, and publish the consolidated transitional list of high impact and critical impact entities on their websites.

4. Within 2 months after entry into force of this Regulation, the ENTSO for Electricity and the EU DSO entity shall develop a transitional list of high-impact and critical-impact processes. The ENTSO for Electricity and the EU DSO entity shall publish the transitional list of processes on their websites. The entities listed in Article 2(1) shall use the transitional list of high-impact and critical-impact processes to determine the transitional high-impact and critical-impact perimeters in order to determine which assets are in the scope of the first cybersecurity risk assessment at entity level.

5. Within 2 months after entry into force of this Regulation the CS-NCAs shall provide a list of relevant national legislation with relevance for cybersecurity aspects of cross-border electricity flows to the ENTSO for Electricity and the EU DSO entity. Within 3 months after entry into force of this Regulation the ENTSO for Electricity and the EU DSO entity shall jointly prepare a transitional list of international standards and controls required by national legislation with relevance for cybersecurity aspects of cross-border electricity flows.

6. The transitional list of international standards and controls shall include:

   (a) international standards and controls stemming from national legislation which provide guidance on methodologies for cybersecurity risk management at entity level;

   (b) cybersecurity controls equivalent to the controls that are expected to be part of the minimum and advanced cybersecurity controls.

7. The ENTSO for Electricity and the EU DSO entity shall jointly consult ENISA, ACER, the NRAs and the CS-NCAs on the proposal for a transitional list of standards. The ENTSO for Electricity and the EU DSO entity shall take into account the views provided by these parties when finalising the transitional list of standards. The ENTSO for Electricity and the EU DSO entity shall publish the transitional list of standards on their websites.

8. Until the minimum and advanced cybersecurity controls are defined, all entities listed in Article 2(1) shall strive to progressively apply the standards and controls included in the transitional list of international standards and controls on the transitional high-impact and critical-impact perimeters defined pursuant to paragraph 4.

Article 50 **Entry into force**

1. This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the Union.

2. This Regulation shall be binding in its entirety and directly applicable in all Member States.

ANNEX A: BASIC CYBERSECURITY HYGIENE REQUIREMENTS

To achieve a minimum level of security the “Review of Cyber Hygiene practices” from the European Union Cybersecurity Agency (ENISA) from September 2017 provide basic cybersecurity hygiene requirements.

Pursuant to Article 2 of this Regulation all entities including micro and small entities shall at least implement the following basic cybersecurity requirements:

- use secure passwords where possible, and keep the passwords safe;
- manage data in and out of their network;
- minimize administrative accounts;
- regularly back up data and test it can be restored;
- establish an incident response plan;
- ensure suitable security controls in service agreements including cloud services;
- raise awareness on common cybersecurity risks such as phishing;
- apply mobile device security;
- apply protection against viruses or other malware on devices exposed to the internet.