entsoe EU DSO entity

Network Code for cybersecurity aspects of cross-border electricity flows

14 January 2022

This document is a draft network code for cybersecurity aspects of cross-border electricity flows (Network Code) submitted by ENTSO-E and EU DSO entity to ACER in accordance with Article 59(9) of Regulation (EU) 2019/943.

The updated draft proposal for this network code reflects the comments received and evaluated by ENTSO-E and EU DSO entity during the public consultation held between 12 November 2021 and 10 December 2021 as well as taking into account the comments from the drafting committee. The draft proposal for the Network Code is in line with the ACER Framework Guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows dated 22 July 2021.

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) Cybersecurity risk management is crucial for maintaining security of electricity supply and for ensuring a high level of cybersecurity in the electricity sector.

(2) Digitalisation and cybersecurity are crucial to provide essential services and therefore of strategic relevance for critical energy infrastructure. This Regulation therefore contributes to the key 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 cybersecurity 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 setting out specific rules for the electricity sector at Union level.

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

(5) Recital (1) and (15) of 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 recognises the vital role of the energy sector for the economy and foresees ENISA to liaise with the European 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'). Their European associations the European network of TSOs for electricity ('ENTSO for Electricity') and the European entity for DSOs ('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 for 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 digitalisation of the electricity sector is progressing rapidly. This Regulation shall not be detrimental to innovation and not constitute a barrier to access the electricity market and the subsequent use of innovative solutions that contribute to the efficiency and sustainability of the electricity system.

(9) The information collected for monitoring the implementation of this Regulation shall be limited to a reasonable amount. Stakeholders shall be granted achievable and effective deadlines for

submitting such information. Double notification should be avoided.

(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 Member States and national institutions should strive to support neighbouring third countries in applying similar cybersecurity rules as set out in this Regulation.

(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 insofar as their activities have a cybersecurity impact directly or indirectly on cross-border electricity flows:

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

   (b) nominated electricity market operators or 'NEMOs' as defined in Article 2(8) of Regulation (EU) 2019/943;

   (c) electricity digital market platforms as defined in Article 4(28) of this Regulation;

   (d) critical service providers as defined in Article 4(12) of this Regulation;

   (e) regional coordination centres or ‘RCCs’ as defined in Article 2(63) and as established pursuant to Article 35 of Regulation (EU) 2019/943;

   (f) the ENTSO for Electricity established pursuant to Article 28 of Regulation (EU) 2019/943;

   (g) the EU DSO entity established pursuant to Article 52 of Regulation (EU) 2019/943;

   (h) the European Union Agency for the Cooperation of Energy Regulators or ‘ACER’ established by Regulation (EU) 2019/942;

   (i) regulatory authorities or ‘NRAs’ as defined in Article 59 of Directive (EU) 2019/944;

(j) national competent authorities for risk preparedness or 'RP-NCA' established pursuant to Article 3 of Regulation (EU) 2019/941;

(k) managed security service provider or 'MSSP' as defined in Article 4(43) of this Regulation;

(l) national competent authorities on the security of network and information systems or 'CS-NCA' as defined in Article 8 of Directive (EU) 2016/1148;

(m) computer security incident response teams or 'CSIRTs' established pursuant to Article 9 of Directive (EU) 2016/1148;

(n) the European Union Agency for Cybersecurity or 'ENISA' established pursuant to Regulation (EU) 2019/881; and

(o) any entity or third party to whom responsibilities have been delegated or assigned.

2. This Regulation shall not apply to micro or small enterprises, or any other entity not listed in Article 2 (1) unless the micro or small 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 16 of this Regulation.

3. This Regulation shall apply to critical service providers not established in the Union but who deliver services to entities in the Union. Where such a critical service provider delivers services to process data, large-scale services and regular services to entities established in the Union, this critical service provider shall explicitly designate a representative in the Union. The representative shall be established in one of those Member States where the services are offered. The critical service provider shall be deemed to be under the jurisdiction of the Member State where the representative is established. 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. In the absence of a designated representative within the Union under this paragraph, any Member State in which the entity provides services may take legal actions against the entity for non-compliance with the obligations under this Regulation. The designation of a representative by an entity referred to in this paragraph shall be without prejudice to legal actions, which could be initiated against the entity itself.

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 electricity system and to ensure close collaboration with existing governance structure(s) for cybersecurity;

(b) determining common criteria for performing risk assessments based on defined risk scenarios for the operational reliability of the electricity system with regard to cross-border electricity flows;

(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 in order to assess the application of the minimum and

advanced 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 resilience and improve the risk preparedness of the electricity sector;

(i) protecting the information exchanged under this Regulation;

(j) determining a process for monitoring the implementation of this Regulation, to assess the effectiveness of investments in cybersecurity protection and to report on the progress of 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, relevant authorities and system operators shall:

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

(b) ensure transparency;

(c) respect the responsibility assigned to the relevant system operator in order to ensure system security;

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

(e) take into consideration agreed European 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 and the definitions in Article 2 of Regulation (EU) 2019/881 apply.

The following definitions also apply:

(1) ‘asset’ means anything that has value to an entity, including business processes, information, hardware, software, networks and sites;

(2) ‘background verification check’ means a verification of the identity and background of staff or contractors of an entity in accordance with relevant laws, regulations, and ethics, which is proportional to business requirements, the classification of the information to be accessed and

the perceived risks. The verification check may be performed by the entity itself, an external company performing a screening, or through a government clearing;

(3) ‘competent authority for cybersecurity’ or ‘CS-NCA’ means a national competent authority responsible for the implementation, monitoring and supervision of cybersecurity at Member State level designated in accordance with Article 8 of Directive (EU) 2016/1148;

(4) ‘competent authority for risk preparedness’ or ‘RP-NCA’ means the competent national authority designated pursuant to 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, as defined in Article 2(13) of Regulation (EC) No 765/2008;

(7) ‘critical-impact asset’ means an asset needed for a critical-impact process;

(8) ‘critical-impact entity’ means an entity that has a critical-impact process or an entity that is a critical service provider as defined in Article 4 (12) of this Regulation;

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

(10) ‘critical-impact process’ means a business process for which the electricity cybersecurity impact indices are above the critical-impact threshold;

(11) ‘critical-impact threshold’ means the values of the electricity cybersecurity impact indices, above which a cyber attack on a process will cause disruption of cross-border electricity flows;

(12) ’critical service provider' means a natural or legal person who provides an ICT product, ICT service, or ICT process that is needed for a critical-impact process, and that if compromised may cause a cybersecurity incident with impact above the critical-impact threshold;

(13) ‘cross border electricity crisis’ means an incident with disruptive effects on cross-border electricity flows, classified by one or more of the affected TSOs as a Scale 2 or 3 electricity incident according to the Incident Classification Scale Methodology of the ENTSO for Electricity;

(14) ‘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 Article 2(3) of Regulation (EU) 2019/943;

(15) ‘CSIRT-NCA’ means the CSIRT or the CS-NCA when designated by the Member State as the competent authority to whom entities shall notify incidents or cyber attacks pursuant to Article 14(3) of Directive (EU) 2016/1148;

(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, as defined in Article 2(1) of Regulation (EU) 2019/881;

(18) ‘cybersecurity-by-design’ means that during the design and development of ICT products, ICT services, and ICT processes, appropriate technical measures for ensuring cybersecurity are considered;

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

(20) ‘cybersecurity operation centre’ or ‘CSOC’ means a team consisting of one or more persons who perform security related tasks (CSOC services) such as handling of incidents and security configuration errors, security monitoring, log analysis, and incident detection;

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

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

(23) ‘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, as defined in Article 2(8) of Regulation (EU) 2019/881;

(24) ‘distribution system operator’ or `DSO` 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 Article 2(29) of Directive (EU) 2019/944;

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

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

(27) ‘electricity cybersecurity impact index’ or ‘ECII’ means the indices for business processes of the electricity sector to estimate the possible consequences of cyber attacks to cross-border electricity flows as defined in Article 16(2)(d);

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

(29) ‘entity’ means any natural or legal person created and recognised as such under the national law of its place of establishment, which may, acting under its own name, exercise rights and be subject to obligations;

(30) ‘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, as defined in Article 2(9) of Regulation (EU) 2019/881;

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

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

(33) ‘high-impact perimeter’ means a 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;

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

(35) ‘high-impact threshold’ means the values of the electricity cybersecurity impact indices defined by the ENTSO for Electricity in cooperation with the EU DSO entity above which a cyber attack on a process could cause disruption of cross-border electricity flows;

(36) ‘ICT product’ means an element or a group of elements of a network or information system as defined in Article 2(12) of Regulation (EU) 2019/881;

(37) ‘ICT process’ means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service as defined in Article 2(14) of Regulation (EU) 2019/881;

(38) ‘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 as defined in Article 2(13) of Regulation (EU) 2019/881;

(39) ‘incident’ means any event, including a cybersecurity incident, compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via network and information systems;

(40) ‘information and communication technology’ or ‘ICT’ means any information being processed digitally by information technology systems and transferred across communication networks;

(41) ‘legacy system’ means a network and information system that cannot always be modified or updated to meet minimum cybersecurity requirements;

(42) ‘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;

(43) ‘managed security service provider’ or ’MSSP’, means any entity which provides outsourced monitoring and management of security devices and systems. Common services include managed firewall, intrusion detection, virtual private network, vulnerability scanning and anti-viral services. It also includes the use of high-availability security operation centres (either from their own facilities or from other data centre providers) to provide 24/7 services designed to reduce the number of operational security personnel an enterprise needs to hire, train and retain to maintain an acceptable security posture.

(44) ‘micro enterprise’ means an enterprise which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 2 million, as defined in Article 2(6) of Directive (EU) 2019/944;

(45) ‘network and information system’ means, pursuant to Article 4(1) of Directive (EU) 2016/1148: (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 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) 'originator' means an entity that initiates an information exchange, information sharing or information storage event;

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

(49) 'regional coordination centre' or 'RCC' means regional coordination centre established pursuant to Article 35 of Regulation (EU) 2019/943;

(50) '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 as defined in Article 4(10) of Directive (EU) 2016/1148;

(51) 'risk impact matrix' means a matrix used during risk assessment to determine the resulting risk impact level for each risk assessed;

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

(53) 'small enterprise' means an enterprise which employs fewer than 50 persons and whose annual turnover and/or annual balance sheet total does not exceed EUR 10 million as defined in Article 2(7) of Directive (EU) 2019/944;

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

(55) 'system operation regions' means the system operation regions as defined in accordance with Article 36 of Regulation (EU) 2019/943;

(56) 'transmission system operator' or `TSO` 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 Article 2(35) of Directive (EU) 2019/944;

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

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

(59) 'vulnerability' means a weakness, susceptibility or flaw of an ICT asset or a system that can be

exploited by a cyber threat;

(60) ‘zero day vulnerability’ means a vulnerability in an 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 disclosed and patched;

(61) ‘zero trust architectures’ means an architecture for network and information systems in which devices (a) are not trusted even when they are within a secure perimeter, (b) verify all requests they receive and (c) apply the least privilege principle.

Article 5. Adoption of terms and conditions or methodologies

1. The ENTSO for Electricity in cooperation with the EU DSO entity shall develop the terms and conditions or 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 or of the EU DSO entity the deadlines for terms and conditions or methodologies may be prolonged by ACER in procedures pursuant to paragraph 4 and jointly by all competent regulatory authorities in procedures pursuant to paragraph 5.
2. Where a proposal for terms and conditions or methodologies pursuant to this Regulation needs to be developed and agreed by more than one TSO or DSO, the participating TSOs and DSOs shall closely cooperate. TSOs, with the assistance of the ENTSO for Electricity, and DSOs, with the assistance of the EU DSO entity, shall regularly inform the competent regulatory authorities and ACER about the progress of developing those terms and conditions or methodologies.
3. If the ENTSO for Electricity in cooperation with the EU DSO entity fails to submit an initial or amended proposal for terms and conditions or methodologies to the competent regulatory authorities or ACER in accordance with paragraphs 4 and 5 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 terms and conditions or methodologies and explain what has prevented an agreement. ACER or all competent regulatory authorities jointly shall take the appropriate steps for the adoption of the required terms and conditions or 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 terms and conditions or methodologies and any amendments thereof shall be subject to approval by ACER:

   (a) the cybersecurity risk assessment methodologies pursuant to Article 16(1);

   (b) the methodology to determine the high-impact and critical-impact perimeters pursuant to Article 16(3);

   (c) the cross-border electricity cybersecurity risk assessment report pursuant to Article 21;

   (d) the minimum and advanced cybersecurity controls and the electricity controls to standards mapping Matrix (ECSMM) pursuant to Article 22;

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

(f) the cybersecurity incidents classification scale methodology pursuant to Article 38(7).

5. The proposal for the regional cybersecurity risk treatment plans pursuant to Article 20 and any amendments thereof shall be subject to approval by all regulatory authorities of the concerned system operation region.

6. The proposal for terms and conditions or methodologies shall include a proposed timescale for their implementation and a description of their expected impact on the objectives of this Regulation. Proposals for terms and conditions or 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 terms and conditions or methodologies.

7. Where the approval of the terms and conditions or 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 terms and conditions or methodologies in accordance with paragraphs 4 and 5 within 6 months following the receipt of the terms and conditions or methodologies by ACER or the regulatory authority or, where applicable, by the last regulatory authority concerned. 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 5.

8. Where the regulatory authorities have not been able to reach agreement within the period referred to in paragraph 7, 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 terms and conditions or 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 request an amendment to approve the terms and conditions or 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 terms and conditions or methodologies for approval within 2 months following the request from ACER or the competent regulatory authorities. ACER or the competent regulatory authorities shall decide on the amended terms and conditions or methodologies within 2 months following their submission. Where the competent regulatory authorities have not been able to reach an agreement on terms and conditions or methodologies pursuant to paragraph 5 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 terms and conditions or 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 terms and conditions or methodologies, the procedure provided for in paragraph 3 of this Article shall apply.

10. ACER, or all competent regulatory authorities jointly, where they are responsible for the adoption of terms and conditions or methodologies in accordance with paragraphs 4 and 5 may respectively request proposals for amendments of those terms and conditions or 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.

11. The proposals for amendment to the terms and conditions or 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.

12. The ENTSO for Electricity in cooperation with the EU DSO entity responsible for establishing the terms and conditions or 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 9.

Article 6. Stakeholder involvement

1. The ENTSO for Electricity in cooperation with the EU DSO entity, shall organise stakeholder involvement via the Working Group pursuant to Article 14. 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 7.

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 that are developed pursuant to Article 5(4)(a).

3. ACER shall organise involvement of other competent authorities at Union and national level via the Monitoring Body pursuant to Article 15. 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 7. Public consultation

1. The ENTSO for Electricity in cooperation with 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)(a), (b), (d) and (f). 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 in cooperation with 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 in cooperation with the EU DSO entity at regional level shall be submitted to public consultation at least at regional level.

3. The ENTSO for Electricity in cooperation with 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 8. Recovery of costs

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

Article 9. Confidentiality obligation

1. Any 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 originator.
2. The obligation of professional secrecy shall apply to any entities subject to the provisions of this Regulation.
3. 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 entity 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 information pursuant to this Regulation may not use it for any other purpose than carrying out its duties under this Regulation.
5. All entities referred to in Article 2 shall provide information, that is necessary for the performance of the tasks referred to in this Regulation, to the concerned entities pursuant to this Regulation.

Article 10. 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 three (3) years and shall:
   (a) assess the contribution of the measures implemented to the three 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;
   (c) identify whether additional measures to the ones laid out in this Regulation may be necessary to prevent risks for the electricity sector; and

(d) 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. Prior to its adoption, ACER shall consult the stakeholders, in particular 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 11. Benchmarking

1. Within 12 months after entry into force of this Regulation ACER, in cooperation with ENISA, shall establish a non-binding cybersecurity benchmarking guide. ACER shall take into account existing benchmarking reports when establishing the non-binding cybersecurity benchmarking guide ACER shall submit the non-binding cybersecurity benchmarking guide to the NRAs.

2. 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 may take into account the non-binding cybersecurity benchmarking guide established by ACER.

   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 with respect to the high-impact entities and to the critical-impact entities; and

   (b) 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.

4. Any information related to benchmarking shall be classified and processed pursuant to data classification requirements of this Regulation, the minimum cybersecurity controls and the cross-

border electricity cybersecurity risk assessment report. The benchmarking pursuant to paragraphs 2 and 3 shall not be made public.

Article 12. Agreements with TSOs not bound by this Regulation

Within 18 months after entry into force of this Regulation, all TSOs of a system operation region that is neighbouring to a third country may endeavour to conclude with the third country TSO(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) with the obligations set out in this Regulation.

Article 13. Cooperation between CS-NCAs, NRAs and CSIRTs of a Member State

1. CS-NCAs and NRAs shall cooperate with each other in carrying out their tasks defined in this Regulation. CS-NCAs and NRAs shall exchange all necessary information and data to carry out their tasks without prejudice to the confidentiality requirements pursuant to Article 9.
2. Where they are separate, the CS-NCA and the CSIRT of the same Member State shall cooperate with each other with regard to the fulfilment of the obligations laid down in Title VIII and X of this Regulation.

TITLE II
GOVERNANCE FOR CYBERSECURITY RISK MANAGEMENT

Article 14. Cybersecurity risk working group

1. Within 3 months after entry into force of this Regulation the ENTSO for Electricity in cooperation with the EU DSO entity shall

   (a) establish a cybersecurity risk working group (hereafter 'the Working Group'); and

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

   The ENTSO for Electricity and the EU DSO entity shall 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 16 (1);

   (b) development of the methodology to determine the high-impact and critical-impact perimeters pursuant to Article 16 (3);

   (c) development of the cross-border electricity cybersecurity risk assessment report pursuant to Article 21;

   (d) development of the common electricity cybersecurity framework pursuant to Article 22;

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

(f) development of the cybersecurity incidents classification scale methodology pursuant to Article 38(7);

(g) development of the transitional electricity cybersecurity impact index pursuant to Article 50(1);

(h) development of the consolidated transitional list of high-impact and critical-impact entities pursuant to Article 50(3);

(i) development of the transitional list of high-impact and critical-impact processes pursuant to Article 50(4);

(j) development of the transitional list of European and international standards and controls pursuant to Article 50(5).

(k) performance of the Union-wide cybersecurity risk assessment pursuant to Article 18;

(l) performance of the regional cybersecurity risk assessments pursuant to Article 19;

(m) definition of the regional cybersecurity risk treatment plans pursuant to Article 20; and

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

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

Article 15. 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 consist 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 10(2)(b); and

(b) adopting the terms and conditions or methodologies pursuant to Article 5(4).

Article 16. 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) metrics to measure the consequences when confidentiality, integrity and availability of information is compromised taking into account safety, operational security, frequency

quality and the efficient use of the interconnected system and resources;

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

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

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

(iii) cyber attacks initiated through actors in the supply chain;

(iv) leaking of sensitive information through the supply chain, including supply chain tracking; and

(v) the introduction of weaknesses or backdoors into ICT products, ICT services, or ICT processes through actors in the supply chain.

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

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

(e) an approach to analyse the cybersecurity risks coming from legacy systems, the cascading effects of 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 in cooperation with 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 in cooperation with the EU DSO entity as well as 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 in cooperation with the EU DSO entity may propose amendments to the cybersecurity risk assessment methodologies.

Article 17. Cybersecurity risk assessment cycle

The cybersecurity risk assessments at Union level, at regional level and at Member State level shall be performed every 3 years. The first risk assessment cycle shall start 24 months after entry into force of this Regulation.

TITLE III
RISK MANAGEMENT AT UNION AND AT REGIONAL LEVEL

Article 18. 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; and

   (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 report 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; and

   (b) 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 9 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. Within 3 months after receipt of ACER's opinion, the ENTSO for Electricity in cooperation with the EU DSO entity shall notify the final report to ACER, ENISA, the Commission, the NIS Cooperation Group, the CS-NCAs, the NRAs, and the RP-NCAs.

Article 19. Regional cybersecurity risk assessments

1. Within 30 months after the start of each risk assessment cycle, 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.

3. The regional cybersecurity risk assessment shall consider the regional electricity crisis scenarios related to cybersecurity identified under the Regulation (EU) 2019 /941.

Article 20. Regional cybersecurity risk treatment and acceptance

1. Within 30 months after the start of each risk assessment cycle, 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 measures the RCC shall apply in the system operation region; and

   (b) the residual cybersecurity risks in the system operation regions after applying the measures referred to in paragraph (a).

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 regional cybersecurity risk treatment plans.

Article 21. Cross-border electricity cybersecurity risk assessment report

1. Within 30 months after the start of each risk assessment cycle, the ENTSO for Electricity in cooperation with 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 assessments;

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

   (c) 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;

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

   (e) status of implementation of the essential information flows pursuant Article 38 and Article 39;

   (f) list of information and/or specific criteria for classification of information per each category of confidentiality level pursuant to Article 47(6);

   (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 risks in the electricity sector since the last regional cybersecurity risk assessments; and

   (j) 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 9.

   The entities listed in Article 2(1) (h), (i), (l) and (n) may contribute to the development of the report.

The ENTSO for Electricity in cooperation with 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 9.

4. Without prejudice to Article 9(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 in cooperation with 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 22. Scope of the common electricity cybersecurity framework

1. Within 30 months are the start of each cybersecurity risk assessment cycle, the ENTSO for Electricity in cooperation with the EU DSO entity shall 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 paragraph 6 and by entities handling the Protected Information pursuant to Article 47;

   (b) advanced cybersecurity controls that shall be applied by all critical-impact entities inside the critical-impact perimeter pursuant to paragraph 6;

   (c) an electricity controls to standards mapping matrix ('ECSMM') that maps the controls from (a) and (b) to selected European and international standards and national legislative frameworks pursuant to Article 29; and

   (d) the cybersecurity management system pursuant to Article 26.

2. The minimum and advanced cybersecurity controls shall include supply chain security controls in accordance with Article 27.

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 24.

4. The minimum and advanced cybersecurity controls shall be based on the risks that are identified in the regional cybersecurity risk assessments.

5. The minimum cybersecurity controls shall include controls to protect the information per each category of information pursuant to Article 47.

6. Within 12 months after the finalisation or update of the minimum and advanced cybersecurity controls, all entities listed in Article 2(1) shall during the risk treatment step pursuant to Article 33(5) apply the minimum cybersecurity controls within the high-impact perimeter and advanced cybersecurity controls within the critical impact perimeter.

Article 23. Derogations from the minimum and advanced cybersecurity controls

1. 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; and

   (b) when 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 33(3)(b).

3. Derogations from the minimum or advanced cybersecurity controls shall be granted for a maximum of three years, renewable. Before granting the derogation the NRAs and the CS-NCAs shall consult the entities that are affected by the derogation. The NRAs and CS-NCAs shall decide whether a derogation is to be granted within 3 months after receipt of the request for a derogation.

4. The list of the derogations, including the information on which ground of paragraph 2 the derogation has been granted, shall be included as an annex to the Cross Border Electricity Cybersecurity Risk Assessment Report. The ENTSO for Electricity in cooperation with the EU DSO entity shall jointly update the list, when necessary.

Article 24. 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 at least one of the following options:

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

   (b) being verified by a national verification scheme.

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

Article 25. Cybersecurity inspections

When exercising their supervisory tasks in relation to high-impact and critical-impact entities, the CS-NCAs may:

(a) carry out on-site inspections and off-site supervision, including random checks; and

(b) request the information necessary to assess the cybersecurity measures adopted by the entity concerned, including the results of the risk assessment at entity level and documented cybersecurity policies.

Article 26. Cybersecurity management system

1. Within 24 months after being notified by the CS-NCA and NRA in accordance with Article 31, all high-impact and critical-impact entities shall establish a cybersecurity management system that is based on a European or international standard and requires entities to:

   (a) determine 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 cybersecurity 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 33;

   (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; and

   (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 27. Minimum and advanced cybersecurity supply chain security controls

1. The ENTSO for Electricity in cooperation with 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 assessments. 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 cybersecurity requirements in the procurement requirements for ICT products, ICT services, and ICT processes covering 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 cybersecurity-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 and restrict access to the entity's 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 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; and

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

(b) only select and contract suppliers that can meet the cybersecurity procurement requirements as stated in paragraph (1) and that possess a level of cybersecurity appropriate to the cybersecurity risks 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; and

(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. For the cybersecurity procurement requirements in paragraph 2(a), entities may use the harmonized cybersecurity procurement requirements in accordance with Article 35, or may define their own requirements based on the results of the cybersecurity risk assessment at entity level.

4. 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 be verified either through a European cybersecurity certification scheme pursuant to Article 36 or through verification activities selected and organized by the entity. The depth and coverage of the verification activities shall be sufficient to provide assurance that the ICT product, ICT service or ICT process can be used to mitigate the risks identified in the risk assessment at entity level. The critical-impact entity shall document the steps taken to reduce the risks identified.

5. The minimum and advanced cybersecurity supply chain security controls in this Article shall apply to ICT product, ICT services, and ICT processes for which the procurement requirements are defined 6 months or more after the finalisation of the minimum and advanced cybersecurity controls.

Article 28. Security measures for critical service providers

1. Critical service providers shall implement processes for secure design, development and production by:
   (a) providing cybersecurity training to their staff;
   (b) ensuring cybersecurity-by-design by considering cyber threats and security requirements; and
   (c) verifying the cybersecurity of an ICT product, ICT service or ICT process through testing, reviews or audits.
2. Critical service providers shall implement vulnerability management, including:
   (a) monitoring vulnerabilities in both internally and externally developed software and hardware, including open-source libraries;
   (b) reporting vulnerabilities to their CSIRT-NCA without undue delay;
   (c) classifying and prioritizing the mitigation of vulnerabilities on objective criteria that reflect their risk to critical-impact processes; and
   (d) providing mitigations for vulnerabilities classified as high-impact under paragraph (c) as soon as possible.
3. Critical service providers shall protect access they have to customer assets and to information that would lead to cybersecurity risks at customers if compromised by:
   (a) performing background verification checks on the staff with access to the assets or to information;
   (b) limiting access to the assets and information to those staff members that need the access to carry out their tasks;
   (c) taking appropriate measures to protect, control and log remote access to customer assets; and
   (d) notifying customers about cybersecurity incidents that may affect them.
4. Critical service providers shall apply the measures in paragraphs (1), (2), and (3) to all processes related to the ICT products, ICT services or ICT processes they provide that are needed for critical-impact processes. The critical service provider shall ensure that the implementation of the measures

is appropriate to the cybersecurity risks.

Article 29. Electricity controls to standards mapping matrix

1. The ENTSO for Electricity in cooperation with the EU DSO entity shall map through the ECSMM the controls set out in Article 22(1)(a) and (b) to selected European and international standards and shall track the conformity of the different controls with the controls set out in Article 22(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 22 (1) (a) and (b) to the national legislative frameworks. If the CS-NCA and NRA of a Member State provide such a mapping, then the ENTSO for Electricity in cooperation with the EU DSO shall integrate the national mapping into the ECSMM.

TITLE V
RISK ASSESSMENT AT MEMBER STATE LEVEL

Article 30. 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 in cooperation with the EU DSO entity in accordance with Article 16. 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 21 months after the start of the cybersecurity risk assessment cycle each CS-NCA supported by the CSIRT 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 implementation status of the minimum and advanced cybersecurity controls;
   (b) recommended additional controls to reduce cybersecurity risks;
   (c) a list of all security incidents reported in the previous 3 years pursuant to Article 39 (2);
   (d) a summary of the cyber threat information reported in the previous 3 years pursuant to Article 39(6);
   (e) for each Union-wide high-impact or critical-impact process, an estimate of the risk of a compromise of the confidentiality, integrity and availability; and
   (f) when necessary, a list of additional entities identified as high-impact or critical-impact pursuant Article 31 (2).
3. The information in the report shall not be linked to specific entities or assets in the report. The estimate of the risk in point (e) shall be given as an estimate of the consequences and likelihood according to the risk-impact matrix.

4. 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 23.

5. The ENTSO for Electricity in cooperation with 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).

6. The CS-NCA shall ensure that the information they provide is accurate, correct, and not older than 21 months.

Article 31. 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. The CS-NCA may request information from an entity to determine the ECII values for the entity. If the ECII of those entities are above the high-impact or critical-impact threshold, the CS-NCA shall use the Union-wide impact assessment report.

2. The CS-NCA may identify additional entities as high-impact or critical-impact entities if the following two criteria are met:

   (a) the entity is part of a group of entities for which there is a significant risk that they will be affected simultaneously by a cyber attack; and

   (b) the ECII aggregated over the group of entities is above the high-impact or critical-impact threshold.

3. If the CS-NCA identifies additional entities in this way, all processes at these entities for which the ECII aggregated over the group are above the high-impact threshold shall be considered high-impact processes. All processes for which the aggregated ECII are above the critical-impact thresholds shall be considered critical impact processes.

4. In each risk assessment cycle, the CS-NCA shall within 9 months after being notified of the Union-wide impact assessment report notify the entities on the list that they have been identified as a high-impact or critical-impact entity.

5. When a service provider is reported to a CS-NCA as being a critical service provider pursuant Article 34 (1)(c), the CS-NCA shall notify it to the CS-NCA of the Member State in whose territory the seat of the critical service provider is situated. The latter CS-NCA shall notify the service provider that it has been identified as being a critical service provider.

Article 32. 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 European and international standards in scope of the verification; and

(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 measures to protect the confidential information they collect during the verification; and

(e) Peer reviews or inspections shall be performed at least once every year and cover the full verification scope at least every three years.

3. If the CS-NCA and the NRA decide to establish a national verification scheme, the CS-NCA and the NRA shall report to ACER on an annual basis how frequently they have performed inspections under the scheme.

TITLE VI
RISK MANAGEMENT AT ENTITY LEVEL

Article 33. 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 paragraph (2) at least every 3 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; and

(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 in cooperation with the EU DSO entity, and other processes that may cause incidents with a high-impact or critical-impact on cross-border electricity flows if compromised by a cyber attack; and

(b) define criteria for risk evaluation and for risk acceptance in accordance with the risk impact matrix defined by the ENTSO for Electricity in cooperation with 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 with an assessment of the possible impact on cross-border electricity flows if the asset is compromised;

(ii) possible cyber threats taking into account the cyber threats identified in the latest Cross-Border Electricity Cybersecurity Risk Assessment Report and supply chain threats;

(iii) vulnerabilities including vulnerabilities in legacy systems;

(iv) possible cybersecurity incident scenarios, including cyber attacks affecting the operational security of the electricity system and disrupting cross-border electricity flows; and

(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 as defined in Article 5 (4)(b); and

(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.

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. The asset inventory shall not be part of the risk assessment report.

8. The CS-NCA and NRA may inspect the asset inventory during on-site inspections pursuant Article 25.

Article 34. Reporting on the risk assessment at entity level

1. Each high-impact and critical-impact entity shall within 12 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 list of controls selected for risk treatment pursuant to Article 33(5) with the current implementation status of each control;

(b) for each Union-wide high-impact or critical-impact process, an estimate of the risk of a compromise of the confidentiality, integrity, and availability; and

(c) a list of critical service providers for the their critical-impact processes.

The controls in (a) shall not be linked to specific assets in the report. The estimate of the risk in (b) shall be given as an estimate of the consequences and likelihood according to the risk impact matrix.

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

3. The entity shall ensure that the information they provide is accurate, correct and from the current cybersecurity risk assessment cycle.

TITLE VII
HARMONISED CYBERSECURITY PROCUREMENT REQUIREMENTS

Article 35. Harmonising cybersecurity procurement requirements

1. The ENTSO for Electricity in cooperation with 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 in cooperation with 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; and

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

2. 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.

3. The harmonised cybersecurity requirement sets shall be based on the outcomes of the cybersecurity risk assessment at regional level. The requirement sets shall be the same for each system operation regions. The sets shall cover at least the topics in Article 27(2)(a). Where possible, the requirements shall be selected from European and international standards.

4. The ENTSO for Electricity in cooperation with the EU DSO entity shall ensure that the cybersecurity procurement requirement sets are compatible with available European cybersecurity certification schemes relevant to the ICT product, ICT service, or ICT process. 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 to be procured.

5. The ENTSO for Electricity in cooperation with the EU DSO entity shall publicly consult the proposal for the harmonised cybersecurity procurement requirements pursuant to Article 7 of this Regulation.

Article 36. Guidance on European cybersecurity certification schemes for ICT products, ICT services and ICT processes

1. 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 in cooperation with 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 profiles with additional testing requirements and rules for determining the exploitability of vulnerabilities.
2. If a suitable European certification scheme is not available, the ENTSO for Electricity in cooperation with 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 paragraph (1). The ENTSO for Electricity in cooperation with the EU DSO entity shall consult the main stakeholders on the guidance in accordance with Article 7. The ENTSO for Electricity in cooperation with the EU DSO entity shall take into account the views provided by all involved stakeholders before finalising the guidance.

TITLE VIII
ESSENTIAL INFORMATION FLOWS, CYBERSECURITY INCIDENT AND CRISIS MANAGEMENT

Article 37. Scope of TITLE VIII

For the essential information flows, cybersecurity incident and crisis management, the national implementation of the Directive (EU) 2016/1148 applies. For cross-border cybersecurity incident and crisis management the additional requirements set out in Title VIII apply.

Article 38. Role of public authorities concerning information sharing

1. CSIRTs shall have the right to share capabilities with other CSIRTs in other Member States following an agreement among the concerned CSIRTs.
2. CSIRTs may delegate fully or partly their responsibilities concerning one or more specific entities that operate in more than one Member State, to another CSIRT. Before delegating such a responsibility to the CSIRT, the concerned entity and the CSIRT of the other Member State shall conclude an agreement to determine at least how and when, the delegating CSIRT shall be kept

informed by the other CSIRT during the delegation period.

3. In the event of a cybersecurity incident notification received from a high-impact or critical impact entity pursuant to Article 39(3), the CSIRT-NCA shall:

   (a) assess the level of confidentiality classification of the information received from the entity, inform the entity about the outcome of its assessment within eighteen (18) hours of receipt of the information and obtain permission to relabel information pursuant to Article 49(3);

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

   (c) be responsible for the sanitisation and the properly anonymization of the relevant information;

   (d) share information with the CSIRT network within eighteen (18) hours after the reception of a reportable cybersecurity incident and provide updated information on a regular basis to the CSIRTs; and

   (e) 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.

4. The CSIRT-NCA receiving the information from the high-impact and the critical-impact entity and the CSIRT-NCAs receiving the information through the CSIRT network shall not disseminate information towards critical impact and high impact entities and shall withhold it as long as the information constitutes a high risk and could harm, hinder or disrupt the investigation of an ongoing cyber attack, or for any other national security consideration.

5. In the event of zero day vulnerability not publicly known received from a high-impact or critical impact entity pursuant to Article 39(4), the CSIRT shall:

   (a) not share any information as long as the critical service provider does not provide the patch or other mitigation measures to the concerned entity; and

   (b) support, with ENISA's guidance, the concerned entity to receive from the vendor an effective and rapid management of the zero day vulnerability.

6. In the event of cyber threats received from a high-impact or critical-impact entity pursuant to Article 39(5), the CSIRT shall disseminate to the CSIRT network and to the entities in its Member State without undue delay information on cyber threats or any other information of importance for preventing, detecting, responding to or mitigating the risk.

7. The ENTSO for Electricity in cooperation with the EU DSO entity and with the support of ENISA and CSIRT network representatives, shall develop a cybersecurity 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 a cybersecurity incident according to 5 levels, the two highest level being 'high' and 'critical';

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

(i) the classification of the asset exposed determined according to Article 33(4) (c); and

(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 in cooperation with 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; and

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

9. The ENTSO for Electricity in cooperation with the EU DSO entity shall:

(a) analyse and facilitate initiatives proposed by entities to test such tools;

(b) consult ENISA, the CSIRT network and the representatives of main stakeholders when assessing the feasibility; and

(c) present the results of the feasibility study to ACER.

Article 39. Role of high-impact and critical-impact entities regarding information sharing

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

(a) establish at least the following CSOC capabilities for all systems within the cybersecurity perimeter of the entity pursuant to Article 33(4)(c):

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

(ii) conducting security monitoring, including but not limited to detecting intrusions and assessing vulnerabilities of network and information systems within the cybersecurity perimeter of the entity pursuant to Article 33(4)(c);

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

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

(b) 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; and

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

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

3. Each critical-impact entity and each high-impact entity shall share any information related to a reportable cybersecurity incident with its CSIRT-NCA no later than four (4) hours after its determination.

A cybersecurity incident shall be considered reportable when the cybersecurity incident is:

(a) sufficiently scoped by the affected entity to determine the cybersecurity incident classification ranging from "high"' to "critical" following the cybersecurity incident classification scale methodology pursuant to Article 38(7); and

(b) the cybersecurity incident classification is confirmed by the authorised representative of the entity.

4. Each critical-impact entity and each high-impact entity shall share any information related to zero day vulnerabilities not publicly known to its CSIRT-NCA, not later than twenty-four (24) hours after its determination by the authorised representative of the entity.

5. Each critical-impact entity and each high-impact entity shall share without undue delay to its CSIRT-NCA any information related to a cyber threat that may have a cross-border effect if the following cybersecurity information is collected in the entity's own environment notwithstanding the success of the cyber attack.

A cyber threat information shall be considered reportable when:

(a) it provides any relevant information for preventing, detecting, responding or mitigating the impact or risk concerning cybersecurity risks; or

(b) the identified artefacts used in the context of an attack, such as compromised URL or IP addresses, hashes or other attributes of malware that are known or can be determined, can be provided.

A cyber threat can be assessed with information provided by service providers or third parties not subjected to this Regulation.

6. Each critical-impact entity and high-impact entity shall, when reporting information pursuant to this Article, specify:

(a) that the information is submitted pursuant to this Regulation;

(b) whether the information concerns:

(i) a reportable cybersecurity incident referred to in paragraph 3;

(ii) zero day vulnerabilities not publicly known referred to in paragraph 4; or

(iii) a cyber-threat referred to in paragraph 5.

(c) in the case of a reportable cybersecurity incident, the level of the cybersecurity incident according to the incident classification scale methodology of the ENTSO for Electricity and

information leading to this classification including at least the criticality of the cybersecurity incident.

7. The reporting of the information required under Article 14(3) of Directive (EU) 2016/1148 constitutes reporting of information compliant with paragraph 6 when it also includes the information listed in paragraph 6(a) to (c).

8. Each critical-impact entity and high-impact entity shall alert its CSIRT-NCA by clearly identifying specific information that shall only be shared with the CSIRT-NCA 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 40. Detection of cybersecurity incidents and handling of cybersecurity incident related information

1. Critical-impact and high-impact entities shall develop the necessary capabilities to handle detected cybersecurity 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 cybersecurity incident and cyber attack and to react rapidly on those flows.

3. In case that a cybersecurity incident has an effect on cross-border electricity flows, the CSOCs or MSSPs of affected critical-impact and high-impact entities shall join their efforts to share information coordinated by the CSIRT-NCA of the Member State in which the cybersecurity incident was reported the first time.

4. Critical-impact and high-impact entities shall:

   (a) report reportable cybersecurity incidents pursuant to Article 39(3);

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

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

   (d) test the overall incident response procedures at least every year by testing at least one scenario affecting directly or indirectly cross-border electricity flows. This annual test may be conducted by critical-impact and high-impact entities during the regular exercises according to Article 44. Any live cybersecurity incident response activities with a consequence classified at least Scale 2 according to the incident classification scale methodology of ENTSO for Electricity with a cybersecurity root cause, can serve as an annual test of the cybersecurity incident response plan.

Article 41. Crisis management

1. Unless otherwise defined by the Member State, the responsibility for crisis management in the event of a cybersecurity incident impacting the cross-border electricity flows rests with the CSIRT-NCA.

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

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

   (a) coordinate the efficient retrieval and further dissemination of all relevant cybersecurity information to the entities involved in the crisis management process;

   (b) organize the communication between all the stakeholders impacted by the crisis including the entities pursuant to paragraph 4 and the CSIRTs, in order to reduce overlaps and increase the efficiency in the analyses and technical responses to remedy the cybersecurity cross-border crisis; and

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

4. On Member State level, CSIRT-NCA shall define the participants in the crisis management process such as 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 and shall provide the necessary support to these entities in order to actively manage the crisis.

Article 42. 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-level cybersecurity crisis management plan and taking into account the national risk preparedness plan established according to Article 10 of Regulation (EU) 2019/941. 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; and

   (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; and

(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 Articles 44 and 45.

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 depending on availability, integrity and reliability of IT services;

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

(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.

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.

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 the reasons to its NRA according to Article 34.

Article 43. 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 the CS-NCAs and relevant research institutions.

2. ENISA shall:

(a) collect voluntary shared information from:

(i) CSIRTs network, CSIRTs and CS-NCAs;

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

(iii) any other entity that wants to share relevant information on a voluntary basis.

(b) assess and classify collected information according to Title X of this Regulation;

(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 CSIRT-NCAs on the identified risks and recommended preventive actions specific to the entities concerned;

(g) inform all entities listed in Article 2(1) on the results of the information assessed pursuant to paragraphs 2(b), (c) and (d);

(h) periodically develop a situational awareness report; and

(i) derive applicable indicators of compromise from the collected information, where possible.

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

4. ACER shall monitor the effectiveness of ECEWC and ENISA shall assist ACER by providing all necessary information. The analysis shall be part of the monitoring pursuant to Article 10.

TITLE IX
ELECTRICITY CYBERSECURITY EXERCISE FRAMEWORK

Article 44. Cybersecurity exercises at entity and Member State level

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

2. By derogation from paragraph 1, the NRA after taking advice from CS-NCA, RP-NCA may decide to organize in a cybersecurity exercise at national level instead of performing the cybersecurity exercise at entity level. In this regard, the NRA shall inform:

(a) all critical-impact entities of its Member and the CS-NCA at the latest by 30 June of the year preceding the cybersecurity exercise at entity level; and

(b) each entity that shall participate in the national exercise 6 months before the exercise takes place.

The NRA with the technical support of CS-NCA, shall organise this national exercise alone, with or under another national cybersecurity exercise. In order to be able to group these exercises, the CS-NCA shall have the authority to deviate from the year referred in paragraph 1, for up to one year.

3. By 31 December [year of publication +1] and every three years afterwards, the ENTSO for Electricity in cooperation with the EU DSO entity, shall make available an exercise scenario template and methodologies to perform the exercise, built on the most recent risk assessment results

performed, for each of the exercises referred to in paragraph 1 and 2, including among other key success criteria. The ENTSO for Electricity in cooperation with the EU DSO entity shall involve ACER and ENISA in the development of the template and the methodology.

Article 45. 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 with 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 cooperation with the EU DSO entity shall inform 6 months before the exercise takes place the entities that shall participate in the exercise.
4. If a regular cybersecurity security exercise at Union level is organised according to Article 7(5) of Regulation (EU) 2019/881 or any mandatory cybersecurity exercise relate to electricity sector within the same geographic perimeter, by derogation from paragraph 1, the organiser of such exercise shall invite the ENTSO for Electricity and the EU DSO entity to participate.
5. If the ENTSO for Electricity in cooperation with the EU DSO entity participate to the exercise in paragraph 4, they can deviate from the usual exercise rhythm pursuant to paragraph 1, for up to one year concerning regional or cross-regional cybersecurity exercises.
6. By 31 December [year of publication +2] and every three years afterwards, the ENTSO for Electricity with the support of EU DSO entity shall make available an exercise template, and methodologies to perform the exercise, built on the most recent risk assessment results , and including among others key success criteria. The ENTSO for Electricity shall involve the Commission and may seek advice from ACER, ENISA and the Joint Research Centre.

Article 46. Internal, national, regional or cross-regional cybersecurity exercises

1. Upon request from a critical-impact entity, critical service providers providing services for the critical-impact entity in the area corresponding with the scope of the exercise, shall participate in the exercises referred in Article 44(1), Article 44(2) and Article 45(1).
2. The cybersecurity exercises organizers, with the advice of ENISA if requested by the organizer, shall analyse and finalize the exercise through a lessons-learnt report addressed to all participants. The lessons-learnt report shall include at least:
   (a) the exercise scenarios, meeting reports, main positions, successes and lessons learnt at any level of the electricity value chain;
   (b) the evaluation of whether the key success criteria were met; and
   (c) a list of recommendations for entities participating in the exercise to correct, adapt or change cybersecurity crisis processes, procedures, associated governance models, and potentially, contractual engagements with critical service providers.

The organizer shall share with each participant information pursuant to paragraphs 2(a) and (b). The organizer shall share the list of recommendations pursuant paragraph 2(c) exclusively with the affected entity addressed.

3. The cybersecurity exercise organizer defined in Article 44 and Article 45 shall follow-up regularly entities participating in the exercises on the implementation of the recommendations pursuant to paragraph 2(c).

TITLE X
PROTECTION OF INFORMATION

Article 47. Basic principles and minimum standards

1. All information, that is listed or meet criteria set forth in the cross-border electricity cybersecurity risk assessment report (’Protected Information’), exchanged among and handled internally by the entities defined in Article 2 shall be protected according to the rules of TITLE X and the information security measures set out in the minimum cybersecurity controls, considering the level of classification of the information applied to the information.

2. 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.

3. 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.

4. Protection of information shall be aimed at protecting confidentiality, integrity, availability and non-repudiation.

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

6. All entities shall classify the Protected Information into the following categories:

   (a) ‘NCCS Classified Information’: information and material that may harm or be disadvantageous to the essential interests of the Union or one or more of its Member States if its confidentiality, integrity or availability are breached;

   (b) ‘NCCS Sensitive Information’: information and material that may harm or be disadvantageous to the essential interests of one or more of the entities listed in Article 2 if its confidentiality, integrity or availability are breached; or

   (c) ‘NCCS Unrestricted Information’: information or material that do not need protection of confidentiality, thus it may be publicly disclosed.

7. Risk management processes set out in this Regulation shall be used to classify information assets and to develop proportionate security measures, procedures and standards, including mitigating measures.

8. The Protected Information shall be classified and reclassified based on the list of information and criteria defined in the cross-border electricity cybersecurity risk assessment report.

9. All systems used to process the Protected Information shall conform with the information security measures foreseen in the minimum cybersecurity controls.

10. In order for an entity defined in Article 2 to classify, handle and receive the Protected Information classified as 'NCCS Classified Information', the entity shall be required to be authorized pursuant to this Regulation by the NRA or CS-NCA of its Member State. The NRA or CS-NCA shall maintain a list of all authorized entities in the Member State.

    (a) For an entity to be authorized, the authorized individual representatives of the entity shall be required to have a security clearance issued by a governmental body mandated by the Union or a Member State. The entity will be required to have a security accreditation of the organization and the information processing systems issued by a governmental body mandated by the Union or a Member State; and

    (b) The rules for authorizing an entity, including the procedures for qualifying an entity for authorization, shall be defined in the minimum cybersecurity controls. Authorization of an entity shall be based on the need for classifying and handling the Protected Information classified as 'NCCS Classified Information' pursuant to this Regulation.

11. When multiple sets of information are aggregated into a single set, the applicable level of classification is equal to the highest level of information category among the original sets.

Article 48. Rules for marking and protecting information

1. Each entity sending the Protected Information shall mark (label) the information with its category name in line with Article 47(6).

2. For the Protected Information marked (labelled) as 'NCCS Classified Information' or 'NCCS Sensitive Information' the sending entity shall mark the 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.

3. For the purpose of this Regulation, the Protected Information not marked (labelled) with a mandatory information category, an identifier of the classifying organization or dissemination label according to paragraphs (1) and (2) by the sending entity shall be handled by the receiving entities pursuant to Title X. In case of reception of non-conformant information, the receiving entity shall inform the sender if identified. If an identified sender does not respond by resending conformant information or by revoking the non-conformant information, or the sender is not identified, the receiving entity shall inform the competent authority depending on the information.

4. All entities shall only exchange 'NCCS Classified Information' and 'NCCS Sensitive Information' internally and externally as part of necessary information processing and following the “need to know” principle. Under “need to know principle” the information can be provided to any other entity or person, only if it is a strict requirement for the actors to fulfil its current role

5. Information to be published shall be restricted to information classified as ‘NCCS Unrestricted Information’ only.

6. Before transferring the ’NCCS Classified Information’ and ’NCCS Sensitive Information’ to entities and persons not bound by this Regulation, an entity referred to in Article 2 shall ensure that these entities and persons are bound by legal obligations in terms of protection of information at least equivalent to this Regulation and the minimum cybersecurity controls.

Article 49. 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 47 and Article 48 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;

   (b) determine the distribution restrictions in accordance with Article 48(2); and

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

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 information categories pursuant to Article 47(6); and

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

3. The CSIRT-NCA receiving information in the context of Title VIII, shall, when needed for sharing the information more widely than indicated by the mark (label) designated pursuant to Article 48(1) and/or 48(2), 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; and

   (b) reclassify 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 CSIRT-NCA after consultation and approval of the organisation classifying the original information.

TITLE XI
FINAL PROVISIONS

Article 50. Transitional provisions

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

2. Within 4 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 ECII 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.

3. Within 6 months after entry into force of this Regulation, the CS-NCAs and the NRAs shall notify the entities on the transitional list that they have been identified as a high-impact or critical-impact entity.

4. Within 2 months after entry into force of this Regulation, the ENTSO for Electricity in cooperation with the EU DSO entity shall develop a transitional list of Union-wide high-impact and critical-impact processes. 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 and 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 in cooperation with the EU DSO entity shall prepare a transitional list of European and international standards and controls required by national legislation with relevance for cybersecurity aspects of cross-border electricity flows.

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

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

   (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 in cooperation with the EU DSO entity shall consult ENISA, ACER, the NRAs and the CS-NCAs on the proposal for a transitional list of standards. The ENTSO for Electricity in cooperation with 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 guidance on cybersecurity risk assessment methodologies and the cybersecurity controls pursuant to paragraph 6 within the transitional high-impact and critical-impact perimeters defined pursuant paragraph 4.

Article 51. 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. By 12 months after the entry into force of this Regulation the essential information flows, cybersecurity incident and crisis management provisions pursuant to Articles 37, 38, 39, 40, 41 and 42 shall be established and operational.

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