Council of the
European Union

Brussels, 13 March 2024
(OR. en)

7721/24

ENER 134
ENV 295
CLIMA 114
COMPET 320
CONSOM 104
FISC 51
CYBER 88
DELACT 55

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	11 March 2024
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	C(2024) 1383 final
Subject:	COMMISSION DELEGATED REGULATION (EU) …/... of 11.3.2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

Delegations will find attached document C(2024) 1383 final.

Encl.: C(2024) 1383 final

EUROPEAN
COMMISSION

Brussels, 11.3.2024
C(2024) 1383 final

COMMISSION DELEGATED REGULATION (EU) …/...

of 11.3.2024

supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

(Text with EEA relevance)

EXPLANATORY MEMORANDUM

1. CONTEXT OF THE DELEGATED ACT

This initiative was identified as an important measure to improve the resilience of critical energy infrastructure and services in Commission communications on energy system integration[1], the Security Union Strategy[2] and the Cybersecurity Strategy[3]. It is based on the powers that the European Parliament and the Council conferred on the Commission in the Regulation (EU) 2019/943[4] (Electricity Regulation) to develop sector-specific rules ('network code') that address the cybersecurity aspects of cross-border electricity flows. This includes rules on common minimum requirements, planning, monitoring, reporting and crisis management

The network code on cybersecurity aspects of cross-border electricity flows will include rules on various electricity cybersecurity-related aspects, such as:

- a comprehensive cross-border risk management process;
- clear roles and responsibilities;
- minimum and advanced cybersecurity controls (mapped against selected European and international standards);
- cybersecurity information sharing flows to ensure timely information and a quick and coordinated response from relevant stakeholders;
- rules on cyber-attack handling and crisis management;
- a cybersecurity exercise framework to strengthen preparedness of all operators;
- rules for the protection of information exchange;
- a framework for monitoring, benchmarking and reporting.

The network code aims to establish a recurrent process of cybersecurity risk assessments in the electricity sector. The assessments will aim to systematically identify the entities that perform digitalised processes with a critical or high impact in cross-border electricity flows, their cybersecurity risks and the necessary mitigating measures that they need to implement. Multiple methodologies and standards exist today in the cybersecurity industry. Moreover, it is a fast-evolving knowledge field. With the objective of harmonising and ensuring a common baseline while respecting existing practices and investments as much as possible, the network code therefore establishes a governance model to develop, follow and regularly review the methodologies of different stakeholders. This governance and stakeholder contribution model takes into account the current mandates of different bodies in both the cybersecurity and electricity regulatory systems.

As technology is constantly evolving and the electricity sector is undergoing rapid digitalisation, the network code therefore strives not to be detrimental to innovation and not to constitute a barrier to new entities accessing the electricity market and the subsequent use of innovative solutions that help make the electricity system more efficient. As part of this

---

1 COM(2020) 299 final
2 COM(2020) 605 final
3 New EU Cybersecurity Strategy
4 Regulation (EU) 2019/943 of the European Parliament and of the Council of 5 June 2019 on the internal market for electricity (recast) (OJ L 158, 14.6.2019, p. 54).

objective, all new systems, processes and procedures must respect cybersecurity requirements. In order to identify new trends and possible future risks in cybersecurity, regular reporting will occur with the comprehensive cross-border electricity cybersecurity risk assessment report, provided for in the network code and carried out at least every 3 years.

The measures envisaged in the network code are important for improving the security of electricity supply in the EU. This delegated Regulation will lay down harmonised rules applicable to all relevant operators in all Member States. It will aim to reach the objectives, while ensuring a level playing field. It will further help integrate the EU electricity market in a non-discriminatory manner and ensure effective competition.

The objectives of this initiative cannot be achieved at national level as it focuses on cross-border electricity flows and refers to interconnected energy networks across Europe.

This Regulation aims at:

- establishing rules concerning the governance of cybersecurity aspects of cross-border electricity flows to ensure the reliability of the electricity system and the close collaboration with existing governance structures for cybersecurity;
- determining common criteria for performing cybersecurity risk assessments for the operational reliability of the electricity system with regard to cross-border electricity flows;
- promoting a common electricity cybersecurity framework and by that fostering a common minimum electricity cybersecurity level across the Union;
- providing for mechanisms in order to assess the application of the minimum and advanced cybersecurity controls on systems that can affect cross-border electricity flows;
- establishing information flows by establishing rules for the collection and sharing of information in relation to cross-border electricity flows, compatible with other national and EU legislation;
- establishing effective processes to identify, classify and respond to cyber-attacks impacting the cross-border flows of electricity;
- setting up effective processes for the management of cross-border electricity crises related to cyber-attacks;
- defining common principles for electricity cybersecurity exercises to increase resilience and improve the risk preparedness of the electricity sector;
- protecting the information exchanged under this Regulation;
- 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; and
- ensuring that the recommendations on the cybersecurity procurement specifications with relevance for cross-border electricity flows are not detrimental to innovation, new systems, processes and procedures.

2. CONSULTATIONS PRIOR TO THE ADOPTION OF THE ACT

Articles 59 and 61 of Regulation (EU) 2019/943 lay down detailed rules on the development of network codes, assigning specific roles to the Agency for the Cooperation of Energy

Regulators (ACER), the European Network of Transmission System Operators for Electricity (ENTSO-E for Electricity) and the entity of the Distribution System Operators for Electricity in the EU (EU DSO entity). It also includes specific rules on detailed consultations of all relevant stakeholders. Articles 31 and 56 lay down requirements for extensive stakeholder consultation when developing the network code.

The network code is the first code being developed based on the new rules established by Regulation (EU) 2019/943, in particular as set out in Article 59. Responsibilities in the formal network code development process are assigned to ENTSO-E, the EU DSO entity and ACER. The network code will be the first code to be (co)drafted by ENTSO-E and the EU DSO entity.

Before the official network code development process was launched, informal work started at the beginning of 2020 under the lead of the Directorate-General for Energy, and concluded with a technical report at the beginning of 2021.

ACER then developed framework guidelines in March-July 2021. The transmission system operators and distribution system operators, with the support of ACER, the Commission and the European Union Agency for Cybersecurity, set up several joint subgroups in March 2021 to develop the technical content of the main areas that were to be covered by the ACER framework guidelines and subsequently the network code. In April 2021, ACER ran a public consultation for 2 months on the draft version of the framework guidelines, inviting stakeholders to share their views. ACER received 42 responses to the consultation, the majority from energy industry companies or associations based within EU Member States. According to ACER, the feedback showed that respondents welcomed the draft framework guidelines; 88% believe the guidelines help further protect cross-border electricity flows; 65% say that there are still gaps in the cybersecurity of cross-border electricity flows, which the draft guidelines should address. Following the feedback received, ACER revised the content of its draft guidelines in consultation with stakeholders, in particular with ENTSO-E and the EU DSO entity, and submitted them to the Commission on 27 July 2021.

The network development process as set out in Article 59 of Regulation (EU) 2019/943 envisages extensive stakeholder involvement as well as a specific drafting committee to help ENTSO-E and the EU DSO entity draft the network code. Pursuant to Article 59(10) of Regulation (EU) 2019/943, ENTSO-E created the drafting committee on 8 September 2021 to kick off the formal drafting process. Taking into consideration the suggestions from the stakeholders listed in Article 59 and in the Commission's letter to ENTSO-E dated 23 July 2021, ENTSO-E formally requested the relevant stakeholders to nominate a representative to the drafting committee in order to participate actively in the monthly meetings and review progress.

ENTSO-E and the EU DSO entity launched a public consultation[5] from 12 November to 10 December 2021 on the draft network code for 1 month. Two public stakeholder workshops were held on 19 November and 8 December 2021. ENTSO-E and the EU DSO entity also held ad hoc meetings and exchanged views with interested parties when necessary. This happened before its final proposal for the network code was submitted to ACER for revision on 14 January 2022.

In January-July 2022, ACER revised the proposed network code to ensure that it complied with the relevant framework guidelines and contributes to market integration, non-

[5] Public consultation: https://www.entsoe.eu/news/2021/11/12/entso-e-and-eu-dso-entity-launch-a-public-consultation-on-the-network-code-on-cybersecurity/

discrimination, effective competition and the efficient functioning of the market. During its revision, ACER conducted extensive consultations with the relevant stakeholders[6] in specific hearings and considered the views provided by all involved parties during the drafting of the proposal led by ENTSO-E and the EU DSO entity.

The Commission has taken into account the comments received and has revised the Delegated Regulation compared to the draft submitted by ACER. In doing so, the Commission also sought assistance from 23 May to 20 June 2023 through timely and appropriate consultations at expert level with the Electricity Coordination Group. This is established in the procedure for the delegated power to adopt measures of general application that supplement or amend certain non-essential elements of Regulation (EU) 2019/943. No vote or formal opinion from the Group was expected. In parallel, the European Parliament and the Council were informed at the same time as Member States' experts, in line with the 2016 Interinstitutional Agreement on Better Law-Making and the Common Understanding on Delegated Acts annexed to it[7]. In addition to consulting the Electricity Coordination Group, DG ENER in cooperation with DG CONNECT and the European Union Agency for Cybersecurity also consulted the Network and Information Systems (NIS) Cooperation Group (workstream on energy). The Commission has completed the next step in the procedure for adoption, after the consultations at expert level with the Electricity Coordination Group. The interservice consultation has been used for requesting and obtaining the formal opinion of other services with a legitimate interest in a draft text. The Commission published the draft Delegated Regulation to the public at large on the Commission's website 'Have your say' for four weeks, from 20 October until 17 November, for all stakeholders to be able to provide feedback. All contributions received are publicly available on the website and the Commission has incorporated the relevant feedback in the text.

3. LEGAL ELEMENTS OF THE DELEGATED ACT

Article 59(2) of Regulation (EU) 2019/943 empowers the Commission to adopt delegated acts in accordance with Article 68 supplementing this Regulation on the establishment of network codes in certain areas.

With respect to cybersecurity, Article 59(2)(e) envisages sector-specific rules for cybersecurity aspects of cross-border electricity flows, including rules on common minimum requirements, planning, monitoring, reporting and crisis management.

Furthermore, Commission Implementing Decision (EU) 2020/1479[8] establishes a priority list for the development of network codes and guidelines for electricity for 2020-2023. Article 1 of that Decision provides for the development of sector-specific rules for cybersecurity aspects of cross-border electricity flows.

Regulation (EU) 2019/941[9] on risk-preparedness in the electricity sector is of utmost importance also for the network code as it requires to put in place appropriate tools to prevent, prepare for and manage possible electricity crises in a spirit of solidarity and transparency. A

---

6 T&D Europe, CSIRT Network, EU DSO entity, SmartEn, NIS workstream on energy, ENTSO-E, NEMOS.

7 Interinstitutional Agreement between the European Parliament, the Council of the European Union and the European Commission on Better Law-Making (OJ L 123, 12.5.2016, p. 1).

8 Commission Implementing Decision (EU) 2020/1479 of 14 October 2020 establishing priority lists for the development of network codes and guidelines for electricity for the period from 2020 to 2023 and for gas in 2020 (OJ L 338, 15.10.2020, p. 10).

9 Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC (OJ L 158, 14.6.2019, p. 1).

cyber-attack could cause, contribute to, or coincide with an electricity crisis as defined in Article 2(9) of Regulation (EU) 2019/941 impacting the cross-border flows of electricity. The network code will build upon existing legal cybersecurity requirements and strive to complement these in order to increase cybersecurity for the electricity sector in the EU. In particular, the general rules on the security of network and information systems laid down in Directive (EU) 2022/2555[10] (NIS 2 Directive) are complemented by the network code. This ensures that cyber-attacks are properly identified as a risk and the measures taken to address them are properly reflected in the risk preparedness plans.

Moreover, the network code was partially drafted while some of the main legislation on cybersecurity was being revised (in particular Directive (EU) 2016/1148, the NIS Directive). All contributors to the drafting of the text have strived to ensure as much coherence, consistency and compatibility as possible with the legislative changes that were discussed in parallel.

Finally, Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) was adopted on 14 December 2022 repealing the former Directive (EU) 2016/1148 (the NIS directive). Directive (EU) 2022/2555 aims to further improve the resilience and incident response capacities of both the public and private sector and the EU as a whole. The network code has therefore been aligned with the new adopted Directive.

[10] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

COMMISSION DELEGATED REGULATION (EU) …/...

of 11.3.2024

supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows

(Text with EEA relevance)

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[11], in particular Article 59 (2), point (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 decisive to provide essential services and therefore of strategic relevance for critical energy infrastructure.

(3) Directive (EU) 2022/2555 of the European Parliament and of the Council[12] lays down measures for a high common level of cybersecurity across the Union. Regulation (EU) 2019/941 of the European Parliament and of the Council[13] complements Directive (EU) 2022/2555 by ensuring that cybersecurity incidents in the electricity sector are properly identified as a risk and that the measures taken to address them are properly addressed in the risk-preparedness plans. Regulation (EU) 2019/943 complements Directive (EU) 2022/2555 and Regulation (EU) 2019/941 by setting out specific rules for the electricity sector at Union level. Furthermore, this Delegated Regulation complements the provisions of Directive (EU) 2022/2555 regarding the electricity sector, whenever cross-border electricity flows are concerned.

(4) In a context of interlinked electricity digitalized systems, prevention and management of electricity crisis related to cyber-attacks cannot be considered to be a solely national task. More efficient and less costly measures through regional and Union cooperation should be developed to its full potential. Therefore, a common framework of rules and better coordinated procedures are needed in order to ensure that Member States and other actors are able to cooperate effectively across borders, in a spirit of increased

[11] OJ L 158, 14.6.2019, p. 54.

[12] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

[13] Regulation (EU) 2019/941 of the European Parliament and of the Council of 5 June 2019 on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC (OJ L 158, 14.6.2019, p. 1).

transparency, trust and solidarity between Member States and competent authorities responsible for electricity and cybersecurity.

(5) Cybersecurity risk management within the scope of this Regulation requires a structured process including, among others, the identification of risks for cross-border flows of electricity stemming from cyber-attacks, the related operational processes and perimeters, the corresponding cybersecurity controls and verification mechanisms. While the timeframe for the whole process is spread over years, each step of it should contribute to a high common level of cybersecurity in the sector and the mitigation of cybersecurity risks. All participants in the process should make their best efforts to develop and agree on the methodologies as soon as possible without undue delay, and in any case, no later than the deadlines defined in this Regulation.

(6) The cybersecurity risk assessments at Union, Member State, regional and entity level in this Regulation may be limited to those resulting from cyber-attacks as defined in Regulation (EU) 2022/2554 of the European Parliament and of the Council[14], therefore excluding, for instance, physical attacks, natural disasters and outages due to loss of facilities or human resources. Union-wide and regional risks related to physical attacks or natural disasters in the electricity domain are already covered by other existing Union legislation, including Article 5 of Regulation 2019/941, or the Commission Regulation (EU) 2017/1485 of 2 August 2017 establishing a guideline on electricity transmission system operation. Similarly, Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities aims to reduce the vulnerabilities and strengthen the physical resilience of critical entities and covers all relevant natural and man-made risks that may affect the provision of essential services, including accidents, natural disasters, public health emergencies such as pandemics, and hybrid threats or other antagonistic threats, including terrorist offences, criminal infiltration and sabotage.

(7) The notion of 'high-impact and critical-impact entities' in this Regulation is fundamental to define the scope of entities that will be subject to the obligations described in this Regulation. The risk-based approach outlined in the different provisions aims to identify the processes, supporting assets and the entities operating them that affect the cross-border electricity flows. Depending on the degree of impact of possible cyber-attacks in their operations of cross-border flows of electricity, they may be considered as 'high-impact' or 'critical-impact'. Article 3 of Directive (EU) 2022/2555 lays down the notions of essential and important entities and the criteria to identify entities with those categories. While many of them will be considered and identified simultaneously as 'Essential' in the sense of Article 3 of Directive (EU) 2022/2555 and high-impact or critical-impact pursuant to Article 24 of this regulation, the criteria laid down in this Regulation refers only to their role and impact in the electricity processes affecting cross-border flows without any consideration to the criteria defined in Article 3 of Directive (EU) 2022/2555.

(8) The entities in the scope of this regulation, considered high-impact or critical-impact pursuant to Article 24 of this Regulation and subject to the obligations laid down

[14] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (OJ L 333, 27.12.2022, p. 1).

therein, are primarily those that have a direct impact on cross-border flows of electricity in the EU.

(9) This Regulation makes use of existing mechanisms and instruments, already established in other legislations, to ensure efficiency and avoid duplication in the achievement of the objectives.

(10) When applying this Regulation, Member States, relevant authorities and system operators should take into consideration agreed European standards and technical specifications of the European Standardisation Organisations and act in line with Union legislation relating to the placing on the market or putting into service of products covered by that Union legislation.

(11) With a view to mitigating cybersecurity risks, it is necessary to establish a detailed rulebook governing the actions of, and the cooperation amongst, relevant stakeholders, whose activities concern cybersecurity aspects of cross-border electricity flows, with the aim of ensuring system security. Those organisational and technical rules should ensure that most electricity incidents with cybersecurity root causes are effectively dealt with at operational level. It is necessary to set out what those relevant stakeholders should do to prevent such crises and what measures they can take should system operation rules alone no longer suffice. Therefore, it is necessary to establish a common framework of rules on how to prevent, prepare for and manage simultaneous electricity crises with a cybersecurity root cause. This brings more transparency in the preparation phase and during a simultaneous electricity crisis and ensures that measures are taken in a coordinated and effective manner together with the competent authorities for cybersecurity in the Member States. Member States and relevant entities should be required to cooperate, at regional level and, where applicable, bilaterally, in a spirit of solidarity. These cooperation and rules are intended to achieve better cybersecurity risk-preparedness at a lower cost, also in line with the objectives of Directive (EU) 2022/2555. It also appears necessary to strengthen the internal electricity market by enhancing trust and confidence across Member States, in particular mitigating the risk of undue curtailment of cross-border flows of electricity, thus reducing the risk of negative spill over effects on neighbouring Member States.

(12) Security of electricity supply entails effective cooperation among Member States, Union institutions, bodies, offices and agencies, and relevant stakeholders. Distribution system operators and transmission system operators play a key role in ensuring a secure, reliable, and efficient electricity system in accordance with Articles 31 and 40 of Directive (EU) 2019/944 of the European Parliament and of the Council[15]. The different regulatory authorities and other relevant competent national authorities also play an important role in ensuring and monitoring the cybersecurity within the electricity supply, as part of their tasks attributed by Directives (EU) 2019/944 and (EU) 2022/2555. Member States should designate an existing or new entity as their competent national authority for the implementation of this Regulation, with the aim of ensuring the transparent and inclusive participation of all actors involved, the efficient preparation and proper implementation of it, the cooperation among the different relevant stakeholders and competent authorities in electricity and cybersecurity, as well as facilitating the prevention and ex post evaluation of

[15] Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity and amending Directive 2012/27/EU (recast) (OJ L 158, 14.6.2019, p. 125).

electricity crises with cybersecurity root causes and information exchanges in relation thereto.

(13) Where a high-impact or critical-impact entity provides services in more than one Member State, or has its seat or other establishment or a representative in a Member State, but its network and information systems are located in one or more other Member States, those Member States should encourage their respective competent authorities to make their best efforts to cooperate with and assist each other as necessary.

(14) Member States should ensure that the competent authorities have the necessary powers, in relation to high-impact and critical-impact entities, to promote compliance with this Regulation. Those powers should allow competent authorities to carry out on-site inspections and off-site supervision. This can include random checks, performing regular audits, targeted security audits based on risk assessments or risk-related available information and security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria and that include requesting information necessary to assess the cybersecurity measures adopted by the entity. That information should include documented cybersecurity policies, access data, documents or any information necessary for the performance of their supervisory tasks, and evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

(15) In order to avoid gaps between or duplications of cybersecurity risk-management obligations imposed on high-impact and critical-impact entities, national authorities under Directive (EU) 2022/2555 and the competent authorities under this Regulation should cooperate in relation to the implementation of cybersecurity risk-management measures and the supervision of compliance with those measures at national level. The compliance of an entity with the cybersecurity risk management requirements laid down in this Regulation could be considered by the competent authorities under Directive (EU) 2022/2555 as ensuring compliance with the corresponding requirements laid down in that Directive, or vice-versa.

(16) A common approach to simultaneous electricity crisis prevention and management requires a common understanding among Member States as to what constitutes a simultaneous electricity crisis consists of and when a cyber-attack is an important factor in it. In particular, coordination among Member States and relevant entities should be facilitated for the purpose of addressing a situation in which the potential risk of a significant electricity shortage or an impossibility to supply electricity to customers is present or imminent, and this due to a cyber-attack.

(17) Recital (1) of Regulation (EU) 2019/881 of the European Parliament and of the Council[16] recognises the vital role of network and information systems and electronic communications networks and services in keeping the economy running in key sectors such as energy, while Recital (44) explains that the European Union Agency for Cybersecurity (’ENISA‘) should liaise with the European Union Agency for the Cooperation of Energy Regulators (‘ACER’).

[16] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

(18) Regulation (EU) 2019/943 assigns specific responsibilities with regard to cybersecurity to Transmission System Operators ('TSOs') and Distribution System Operators ('DSOs'). Their European associations, namely the European network of TSOs for electricity ('ENTSO for Electricity') and the European entity for DSOs ('EU DSO entity') shall, pursuant to Articles 30 and 55 of that Regulation respectively, promote cybersecurity in cooperation with relevant authorities and regulated entities.

(19) A common approach to prevention and management of simultaneous electricity crises with cybersecurity root causes also requires that all relevant stakeholders use harmonised methods and definitions to identify risks relating to the cybersecurity of electricity supply. It also requires to be in a position to compare effectively how well they and their neighbours perform in that area. Therefore, it is necessary to establish the processes and roles and responsibilities to develop and update risk management methodologies, incident classification scales and cybersecurity measures adapted to the cybersecurity risks impacting the cross-border flows of electricity.

(20) Member States through the competent authority designated for this Regulation are responsible for identifying the entities which meet the criteria to qualify as high-impact and critical-impact entities. In order to eliminate divergences among Member States in that regard and ensure legal certainty as regards the cybersecurity risk-management measures and reporting obligations for all relevant entities, a set of criteria should be established that determines the entities falling within the scope of this Regulation. That set of criteria should be defined and regularly updated through the development and adoption process of terms, conditions and methodologies laid down in this Regulation.

(21) The provisions of this Regulation should be without prejudice to Union law providing for specific rules on the certification of information and communication technology ('ICT') products, ICT services and ICT processes, in particular without prejudice to Regulation (EU) 2019/881 with regard to the framework for the establishment of European cybersecurity certification schemes. In the context of this Regulation, ICT products should also include technical devices and software that enable direct interaction with the electrotechnical network, in particular industrial control systems that can be used for energy transmission, energy distribution and energy production, as well as for the collection and transmission of related information. The provisions should ensure that the relevant security objectives in Article 51 of Regulation (EU) 2019/881 are met by the ICT products, ICT services and ICT processes to be procured.

(22) Recent cyber-attacks show that entities are increasingly becoming the target of supply chain attacks. Such supply chain attacks not only have an impact on individual entities in the scope but can also have a cascading effect on larger attacks on entities to which they are connected in the electricity grid. Provisions and recommendations to help mitigate the cybersecurity risks associated to processes related to the supply chain, notably procurement, with impact on the cross-border flows of electricity have therefore been added.

(23) Since the exploitation of vulnerabilities in network and information systems may cause significant energy disruptions and harm for economy and consumers, these vulnerabilities should be swiftly identified and remedied in order to reduce risks. In order to facilitate the effective implementation of this Regulation relevant entities and competent authorities should cooperate to exercise and test activities that are considered to be appropriate for that purpose, including information exchange on cyber threats, cyber-attacks, vulnerabilities, tools and methods, tactics, techniques and

procedures, cybersecurity crisis management preparedness and other exercises. Since technology is evolving constantly and digitalisation of the electricity sector is progressing rapidly, the implementation of the provisions adopted should 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.

(24) The information collected in view of monitoring the implementation of this Regulation should be reasonably limited on a need-to-know principle. Stakeholders should be granted achievable and effective deadlines for submitting such information. Double notification should be avoided.

(25) Cybersecurity protection does not stop at the Union's borders. A secure system requires the involvement of neighbouring third countries. The Union and its Member States should strive to support neighbouring third countries whose electricity infrastructure is connected to the European grid in applying similar cybersecurity rules as set out in this Regulation.

(26) In order to improve security coordination early on, to test future binding terms, conditions and methodologies, the ENTSO for Electricity, the EU DSO Entity and the competent authorities should start developing non-binding guidance immediately after the entry into force of this Regulation. This guidance will serve as a baseline for the development of the future terms, conditions and methodologies. In parallel, the competent authorities should identify entities as candidates to high- and critical-impact entities to start, on a voluntary basis, to fulfil the obligations.

(27) This Regulation has been developed in close cooperation with ACER, ENISA, the ENTSO for Electricity, the EU DSO entity and other stakeholders, in order to adopt effective, balanced and proportionate rules in a transparent and participative manner.

(28) This Regulation complements and enhances the crisis management measures established in the EU Cybersecurity Crisis Response Framework, as set out in Commission Recommendation (EU) 2017/1584[17]. A cyber-attack could also cause, contribute to, or coincide with an electricity crisis as defined in Article 2(9) of Regulation (EU) 2019/941, impacting the cross-border flows of electricity. That electricity crisis could lead to a simultaneous electricity crisis as defined in Article 2(10) of Regulation (EU) 2019/941. Such an incident could also have an impact on other sectors dependent on the security of electricity supply. Should such an incident escalate to a large-scale cybersecurity incident within the meaning of Article 16 of Directive (EU) 2022/2555, provisions in that Article establishing the European cyber crisis liaison organisation network (’EU-CyCLONe’) should apply. For crisis management at Union level, relevant parties should rely on the EU Integrated Political Crisis Response arrangements (’IPCR arrangements’) under Council Implementing Decision (EU) 2018/1993[18].

(29) This Regulation is without prejudice to the competence of Member States to take the necessary measures to ensure the protection of the essential interests of their security, to safeguard policy and public security, and to allow for the investigation, detection and prosecution of criminal offences, in compliance with Union law. In accordance

[17] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

[18] Council Implementing Decision (EU) 2018/1993

with Article 346 TFEU, no Member State is to be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security.

(30) Although this Regulation applies, in principle, to entities carrying out activities in the production of electricity from nuclear power plants, some of those activities may be linked to national security.

(31) Union data protection law and Union privacy law should apply to any processing of personal data under this Regulation. In particular, this Regulation is without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council[19], Directive 2002/58/EC of the European Parliament and of the Council[20] and Regulation (EU) 2018/1725 of the European Parliament and of the Council[21]. This Regulation should therefore not affect, inter alia, the tasks and powers of the authorities competent to monitor compliance with the applicable Union data protection law and Union privacy law.

(32) Given the importance of international cooperation on cybersecurity, the competent authorities responsible for carrying out the tasks assigned to them under this Regulation and designated by Member States should be able to participate in international cooperation networks. Therefore, for the purpose of carrying out their tasks, the competent authorities should be able to exchange information, including personal data, with the competent authorities of third countries provided that the conditions under Union data protection law for transfers of personal data to third countries, inter alia those of Article 49 of Regulation (EU) 2016/679, are met.

(33) The processing of personal data, to the extent necessary and proportionate for the purpose of ensuring security of assets by high-impact or critical-impact entities, could be considered to be lawful on the basis that such processing complies with a legal obligation to which the controller is subject, in accordance with the requirements of Article 6(1), point (c), and Article 6(3) of Regulation (EU) 2016/679. Processing of personal data may also be necessary for legitimate interests pursued by high-impact or critical-impact entities, as well as providers of security technologies and services acting on behalf of those entities, pursuant to Article 6(1), point (f), of Regulation (EU) 2016/679, including where such processing is necessary for cybersecurity information-sharing arrangements or the voluntary notification of relevant information in accordance with this Regulation. Measures related to the prevention, detection, identification, containment, analysis and response to cyber-attacks, measures to raise awareness in relation to specific cyber threats, exchange of information in the context of vulnerability remediation and coordinated vulnerability disclosure, the voluntary exchange of information about those cyber-attacks, and cyber threats and vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts and configuration tools may require the processing of certain categories of personal data, such as IP addresses, uniform resources locators (URLs), domain names, email addresses and, where they reveal personal data, time stamps. Processing of personal data by the competent authorities, the single points of contact and the CSIRTs, may constitute a legal obligation or be considered to be necessary for carrying out a task in the public interest or in the exercise of official authority vested in the controller pursuant to Article 6(1), point (c) or (e), and Article 6(3) of

19 Regulation (EU) 2016/679
20 Directive 2002/58/EC
21 Regulation (EU) 2018/1725

Regulation (EU) 2016/679, or for pursuing a legitimate interest of the high-impact or critical-impact entities, as referred to in Article 6(1), point (f), of that Regulation. Furthermore, national law may lay down rules allowing the competent authorities, the single points of contact and the CSIRTs, to the extent that is necessary and proportionate for the purpose of ensuring the security of network and information systems of high-impact or critical-impact entities, to process special categories of personal data in accordance with Article 9 of Regulation (EU) 2016/679, in particular by providing for suitable and specific measures to safeguard the fundamental rights and interests of natural persons, including technical limitations on the re-use of such data and the use of state-of-the-art security and privacy-preserving measures, such as pseudonymisation, or encryption where anonymisation may significantly affect the purpose pursued.

(34) Personal data are in many cases compromised as a result of cyber-attacks. In that context, the competent authorities should cooperate and exchange information about all relevant matters with the authorities referred to in Regulation (EU) 2016/679 and Directive 2002/58/EC.

(35) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 and delivered an opinion on 17 November 2023,

HAS ADOPTED THIS REGULATION:

Chapter 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. This Regulation applies to cybersecurity aspects of cross-border electricity flows in the activities of the following entities, if they are identified as high-impact or critical-impact entities in accordance with Article 24:

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

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

(c) organised market places or 'organised markets' as defined in Article 2(4) of Commission Implementing Regulation (EU) No 1348/2014[22] that arrange transactions on products relevant to cross-border electricity flows;

(d) critical ICT service providers as referred to in Article 3, point (9) of this Regulation;

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

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

(g) balancing responsible parties as defined in Article 2, point (14) of Regulation (EU) 2019/943

(h) operators of recharging points as defined in Annex I to Directive (EU) 2022/2555;

(i) regional coordination centres ('RCCs') as established pursuant to Article 35 of Regulation (EU) 2019/943;

(j) managed security service providers ('MSSP') as defined in Article 6(40) of Directive (EU) 2022/2555;

(k) any other entity or third party to whom responsibilities have been delegated or assigned pursuant to this Regulation.

2. The following authorities are, as part of their current mandates, responsible to perform tasks assigned in this Regulation:

(a) the European Union Agency for the Cooperation of Energy Regulators ('ACER') established by Regulation (EU) 2019/942;

(b) national competent authorities responsible for carrying out the tasks assigned to them under this Regulation and designated by Member States pursuant to Article 4, or 'competent authority';

(c) national regulatory authorities ('NRAs') designated by each Member State pursuant to Article 57(1) of Directive (EU) 2019/944;

(d) competent authorities for risk preparedness ('RP-NCAs') established pursuant to Article 3 of Regulation (EU) 2019/941;

(e) computer security incident response teams ('CSIRTs') as designated or established pursuant to Article 10 of Directive (EU) 2022/2555;

(f) competent authorities responsible for cybersecurity ('CS-NCAs') as designated or established pursuant to Article 8 of Directive (EU) 2022/2555;

(g) the European Union Agency for Cybersecurity established pursuant to Regulation (EU) 2019/881;

(h) any other authorities or third party to whom responsibilities have been delegated or assigned pursuant to Article 4(3).

[22] Commission Implementing Regulation (EU) No 1348/2014 of 17 December 2014 on data reporting implementing Article 8(2) and Article 8(6) of Regulation (EU) No 1227/2011 of the European Parliament and of the Council on wholesale energy market integrity and transparency (OJ L 363, 18.12.2014, p. 121).

3. This Regulation shall also apply to all entities who are not established in the Union but who deliver services to entities in the Union, provided they have been identified as high or critical-impact entities by the competent authorities in accordance with Article 24(2).

4. This Regulation is without prejudice to the Member States' responsibility for safeguarding national security and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.

5. This Regulation is without prejudice to the Member States' responsibility for safeguarding national security with respect to activities in the production of electricity from nuclear powers plants, including activities within the nuclear value chain, in accordance with the Treaties.

6. Entities, the competent authorities, the single points of contact at entity level and the CSIRTs shall process personal data to the extent necessary for the purposes of this Regulation and in accordance with Regulation (EU) 2016/679, in particular such processing shall rely on Article 6 thereof.

Article 3

Definitions

The following definitions apply:

(1) 'asset' means any information, software or hardware in the network and information systems either tangible or intangible, that has value to an individual, an organization or a government;

(2) 'competent authority for risk preparedness' means the competent authority designated pursuant to Article 3 of Regulation (EU) 2019/941;

(3) 'computer security incident response team' means a team responsible for risk and incident handling in accordance with Article 10 of Directive (EU) 2022/2555;

(4) 'critical-impact asset' means an asset that is necessary to carry out a critical-impact process;

(5) 'critical-impact entity' means an entity that carries out a critical-impact process and that is identified by the competent authorities in accordance with Article 24;

(6) 'critical-impact perimeter' means a perimeter defined by an entity referred to in Article 2(1) that contains all critical-impact assets and on which access to these assets can be controlled and that defines the scope where the advanced cybersecurity controls apply;

(7) 'critical-impact process' means a business process carried out by an entity for which the electricity cybersecurity impact indices are above the critical-impact threshold;

(8) 'critical-impact threshold' means the values of the electricity cybersecurity impact indices referred to in Article 19(3)b, above which a cyber-attack on a business process will cause critical disruption of cross-border electricity flows;

(9) 'critical ICT service provider' means an entity which provides an ICT service, or ICT process that is necessary for a critical-impact or high-impact process affecting

cybersecurity aspects of cross-border electricity flows and that, if compromised, may cause a cyber-attack with impact above the critical-impact or high-impact threshold;

(10) ‘cross-border electricity flow’ means a cross-border flow as defined in Article 2(3) of Regulation (EU) 2019/943;

(11) ‘cyber-attack’ means an incident as defined in Article 3, point (14), of Regulation (EU) 2022/2554;

(12) ‘cybersecurity’ means cybersecurity as defined in Article 2, point (1) of Regulation (EU) 2019/881;

(13) ‘cybersecurity control’ means the actions or procedures carried out with the purpose of avoiding, detecting, counteracting, or minimizing cybersecurity risks;

(14) ‘cybersecurity incident’ means an incident as defined in Article 6, point (6) of Directive (EU) 2022/2555;

(15) ‘cybersecurity management system’ means the policies, procedures, guidelines, and associated resources and activities, collectively managed by an entity, in the pursuit of protecting its information assets from cyber threats systematically establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organisation’s network and information system security;

(16) ‘cybersecurity operation centre’ means a dedicated centre where a technical team consisting of one or more experts, supported by cybersecurity IT systems, performs security-related tasks (Cybersecurity operation center (‘CSOC’) services) such as handling of cyber-attacks and security configuration errors, security monitoring, log analysis, and cyber-attack detection;

(17) ‘cyber threat’ means a cyber threat as defined in Article 2, point (8) of Regulation (EU) 2019/881;

(18) 'cybersecurity vulnerability management’ means the practice of identifying and addressing vulnerabilities;

(19) ‘entity’ means entity as defined in Article 6, point (38) of Directive (EU) 2022/2555;

(20) ‘early alert’ means the information necessary to indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

(21) ‘electricity cybersecurity impact index’ (‘ECII’) means an index or classification scale that ranks possible consequences of cyber-attacks to business processes involved in cross-border electricity flows;

(22) ‘European cybersecurity certification scheme’ means a scheme as defined in Article 2, point (9) of Regulation (EU) 2019/881;

(23) ‘high-impact entity’ means an entity that carries out a high-impact process and that is identified by the competent authorities in accordance with Article 24;

(24) ‘high-impact process’ means any business process carried out by an entity for which the electricity cybersecurity impact indices are above the high-impact threshold;

(25) ‘high-impact asset’ means an asset that is necessary to carry out a high-impact process;

(26) ‘high-impact threshold’ means the values of the electricity cybersecurity impact indices referred to in Article 19(3)b, above which a successful cyber-attack on a process will cause high disruption of cross-border electricity flows;

(27) ‘high-impact perimeter’ means a perimeter defined by any entity listed in Article 2(1) that contains all high-impact assets and on which access to these assets can be controlled and that defines the scope where the minimum cybersecurity controls apply;

(28) ‘ICT product’ means an ICT product as defined in Article 2 point (12) of Regulation (EU) 2019/881;

(29) ‘ICT service’ means an ICT service as defined in Article 2 point (13) of Regulation (EU) 2019/881;

(30) ‘ICT process’ means an ICT process as defined in Article 2 point (14) of Regulation (EU) 2019/881;

(31) ‘legacy system’ means a legacy ICT system as defined in Article 3(3) of Regulation (EU) 2022/2554;

(32) ‘national single point of contact’ means the single point of contact designated or established by each Member State pursuant to Article 8(3) of Directive (EU) 2022/2555;

(33) ‘NIS cyber crisis management authorities’ means the authorities designated or established pursuant to Article 9, point (1) of Directive (EU) 2022/2555;

(34) ‘originator’ means an entity that initiates an information exchange, information sharing or information storage event;

(35) ‘procurement specifications’ means the specifications that entities define for the procurement of new or updated ICT products, ICT processes or ICT services;

(36) ‘representative’ means a natural or legal person established in the Union who is explicitly designated to act on behalf of a high or critical-impact entity not established in the Union but delivering services to entities in the Union and who may be addressed by a competent authority or a CSIRT in the place of the high or critical-impact entity itself with regard to the obligations of that entity under this Regulation;

(37) ‘risk’ means risk as defined in Article 6, point (9) of Directive (EU) 2022/2555;

(38) ‘risk impact matrix’ means a matrix used during risk assessment to determine the resulting risk impact level for each risk assessed;

(39) ‘simultaneous electricity crisis’ means an electricity crisis as defined in Article 2, point (10) of Regulation (EU) 2019/941;

(40) ‘single point of contact at entity level’ means single point of contact at entity level as designated under Article 38(1) point (c);

(41) ‘Stakeholder’ is any party that has an interest in the success and ongoing operation of an organisation or process such as employees, directors, shareholders, regulators, associations, suppliers and customers;

(42) ‘standard’ means a standard as defined in Article 2(1) of Regulation (EU) No 1025/2012;

(43) ‘system operation region’ means the system operation regions as defined in Annex I to ACER Decision 05-2022 on the Definition of System Operation Regions, established in accordance with Art. 36 of Regulation 2019/943;

(44) ‘system operators’ means ‘distribution system operator’ (DSO) and ‘transmission system operator’ (TSO) as defined in Articles 2 (29) and 2(35) of Directive (EU) 2019/944;

(45) ‘Union-wide critical-impact process’ means any electricity sector process, possibly involving multiple entities, for which the possible impact of a cyber-attack may be deemed critical during the performance of the Union-wide cybersecurity risk assessment;

(46) ‘Union-wide high-impact process’ means any electricity sector process, possibly involving multiple entities, for which the possible impact of a cyber-attack may be deemed high during the performance of the Union-wide cybersecurity risk assessment;

(47) ‘unpatched actively exploited vulnerability’ means a vulnerability, which has not yet been publicly disclosed and patched and for which there is reliable evidence that execution of malicious code was performed by an actor on a system without permission of the system owner;

(48) ‘vulnerability’ means a vulnerability as defined in Article 6, point (15) of Directive (EU) 2022/2555.

Article 4

Competent authority

1. As soon as possible and in any event by [*OP: please insert the date = six months after entry into force of this Regulation*], each Member State shall designate a national governmental or regulatory authority responsible for carrying out the tasks assigned to it in this Regulation (‘competent authority’). Until the competent authority has been assigned with carrying out the tasks under this Regulation, the regulatory authority designated by each Member State pursuant to Article 57(1) of Directive (EU) 2019/944 shall carry out the tasks of the competent authority in accordance with this Regulation.

2. Member States shall, without delay, notify the Commission, ACER, ENISA, the NIS Cooperation Group established pursuant to Article 14 of Directive (EU) 2022/2555 and the Electricity Coordination Group set up under Article 1 of Commission Decision of 15 November 2012[23] and communicate to them the name and the contact details of their competent authority designated pursuant to paragraph 1 of this article and any subsequent changes thereto.

3. Member States may allow their competent authority to delegate tasks assigned to it in this Regulation to other national authorities with the exception of the tasks listed in Article 5. Each competent authority shall monitor the application of this Regulation by the authorities to whom it has delegated tasks. The competent authority shall communicate the name, contact details, assigned tasks and any subsequent changes

[23] Commission Decision of 15 November 2012 setting up the Electricity Coordination Group (OJ C 353, 17.11.2012, p. 2).

thereto of the authorities to whom a task has been delegated to the Commission, to ACER, to the Electricity Coordination Group, to ENISA and to the NIS Cooperation Group.

Article 5

Cooperation between relevant authorities and bodies at national level

The competent authorities shall coordinate and ensure appropriate cooperation between the competent authorities responsible for cybersecurity, the cyber crisis management authorities, the NRAs, competent authorities for risk preparedness and CSIRTs for the purpose of the fulfilment of the relevant obligations laid down in this Regulation. The competent authorities shall also coordinate with any other bodies or authorities as determined by each Member State, to ensure efficient procedures and avoid duplications of tasks and obligations. The competent authorities shall be able to instruct the respective NRAs to request ACER for an opinion pursuant to Article 8(3).

Article 6

Terms and conditions or methodologies or plans

1. TSOs shall develop, in cooperation with the EU DSO entity, proposals for the terms and conditions or methodologies pursuant to paragraph 2, or for plans pursuant to paragraph 3.
2. The following terms and conditions or methodologies and any amendments thereof shall be subject to approval by all competent authorities:
   (a) the cybersecurity risk assessment methodologies pursuant to Article 18(1);
   (b) the Comprehensive Cross-border electricity cybersecurity risk assessment report pursuant to Article 23;
   (c) the minimum and advanced cybersecurity controls pursuant to Article 29, the mapping of electricity cybersecurity controls against standards pursuant to Article 34, including minimum and advanced cybersecurity controls in the supply chain in accordance with Article 33;
   (d) a cybersecurity procurement recommendation pursuant to Article 35;
   (e) the cyber-attacks classification scale methodology pursuant to Article 37(8).
3. The proposals for the regional cybersecurity risk mitigation plans pursuant to Article 22 shall be subject to approval by all competent authorities of the concerned system operation region.
4. The proposals for terms and conditions, methodologies listed in paragraph 2, or for plans listed in paragraph 3, shall include a proposed timescale for their implementation and a description of their expected impact on the objectives of this Regulation.
5. The EU DSO entity may provide a reasoned opinion to the concerned TSOs until 3 weeks before the deadline to submit the proposal for terms and conditions or methodologies or plans to the competent authorities. TSOs responsible for the proposal for terms and conditions or methodologies or plans shall take into consideration the reasoned opinion of the EU DSO entity prior to its submission for

competent authorities' approval. TSOs shall provide reasoning where the EU DSO entity opinion is not taken into account.

6. When jointly developing terms, conditions and methodologies and plans, the participating TSOs shall closely cooperate. TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall regularly inform competent authorities and ACER about the progress of developing the terms and conditions or methodologies, or plans.

Article 7

Voting rules in the TSOs

1. Where TSOs deciding on proposals for terms and conditions or methodologies are not able to reach an agreement, they shall decide by qualified majority voting. A qualified majority for such proposals shall be calculated as follows:

   (a) TSOs representing at least 55 % of the Member States; and

   (b) TSOs representing Member States comprising at least 65 % of the population of the Union.

2. A blocking minority for decisions on proposals for terms and conditions or methodologies listed in Article 6(2) shall include TSOs representing at least four Member States, failing of which the qualified majority shall be deemed attained.

3. Where TSOs of a system operation region deciding on proposals for plans listed in Article 6(2) are not able to reach an agreement, and where the system operation region concerned is composed of more than five Member States, TSOs shall decide by qualified majority voting. A qualified majority for proposals listed in Article 6(2) shall require the following majority:

   (a) TSOs representing at least 72 % of the Member States concerned; and

   (b) TSOs representing Member States comprising at least 65 % of the population of the concerned area.

4. A blocking minority for decisions on proposals for the plans shall include at least a minimum number of TSOs representing more than 35 % of the population of the participating Member States, plus TSOs representing at least one additional Member State concerned, failing of which the qualified majority shall be deemed attained.

5. For TSO decisions on proposals for terms and conditions or methodologies pursuant to Article 6(2), one vote shall be attributed per Member State. If there is more than one TSO in the territory of a Member State, the Member State shall allocate the voting powers among the TSOs.

6. If TSOs, in cooperation with the EU DSO entity, fail to submit an initial or amended proposal for terms and conditions or methodologies, or for plans, to the relevant competent authorities within the deadlines set out in this Regulation, they shall provide the relevant competent authorities and ACER with the relevant drafts of the terms and conditions or methodologies, or of the plans. They shall explain what has prevented an agreement. The competent authorities shall jointly take the appropriate steps for the adoption of the required terms and conditions or methodologies, or of the required plans. This may be done for instance by requesting amendments to the drafts pursuant to this paragraph, by revising and completing those drafts, or, where

no drafts have been provided, by defining and approving the required terms and conditions or methodologies or plans.

Article 8

Submission of proposals to the competent authorities

1. TSOs shall submit the proposals for terms and conditions or methodologies, or for plans for approval to the relevant competent authorities within the respective deadlines set out in Articles 18, 23, 29, 33, 34, 35 and 37. The competent authorities may jointly prolong these deadlines in exceptional circumstances, notably in cases where a deadline cannot be met due to circumstances external to the sphere of TSOs or of the EU DSO entity.
2. Proposals for terms and conditions, methodologies or for plans pursuant to paragraph 1, shall be submitted for information to ACER at the same time that they are submitted to the competent authorities.
3. Upon a joint request of the NRAs, ACER shall issue an opinion on the proposal for terms and conditions or methodologies, or for the plans, within six months of the receipt of the proposals for terms and conditions or methodologies, or for plans and notify NRAs and competent authorities of the opinion. NRAs, CS-NCAs and any other authorities designated as competent authorities shall coordinate with each other before the NRAs requests an opinion to ACER. ACER may include recommendations in such opinion. ACER shall consult ENISA before issuing an opinion on the proposals listed in Article 6(2).
4. The competent authorities shall consult and closely cooperate and coordinate with each other in order to reach an agreement on the proposed terms and conditions, methodologies, or plans. Before approving the terms and conditions or methodologies, or the plans, they shall revise and complete the proposals where necessary, after consulting the ENTSO for Electricity and the EU DSO entity, in order to ensure that the proposals are in line with this Regulation and contribute to a high common level of cybersecurity across the Union.
5. The competent authorities shall decide on the terms and conditions or methodologies or on the plans within six months following the receipt of the terms and conditions or methodologies or of the plans by the relevant competent authority or, where applicable, by the last relevant competent authority concerned.
6. Where ACER issues an opinion, the relevant competent authorities shall take that opinion into account and shall take their decisions within six months from the receipt of ACER's opinion.
7. Where the competent authorities jointly require an amendment to the proposed terms and conditions or methodologies, or the plans, in order to approve them, the TSOs shall develop, in cooperation with the EU DSO entity, a proposal for such amendment to the terms and conditions or methodologies, or the plans. The TSOs shall submit the amended proposal for approval within two months following the request of the competent authorities. The competent authorities shall decide on the amended terms and conditions or methodologies, or plans, within two months following their submission.

8. Where the competent authorities have not been able to reach an agreement within the period referred to in paragraph 5 or 7, they shall inform the Commission. The Commission may take appropriate steps to make possible the adoption of the required terms and conditions or methodologies, or plans.

9. TSOs, with the assistance of the ENTSO for Electricity, and the EU DSO entity shall publish the terms and conditions or methodologies, or the plans, on their websites following approval by the relevant competent authorities, except where such information is considered as confidential in accordance with Article 47.

10. The competent authorities may jointly request proposals for amendments of the approved terms and conditions or methodologies, or of the approved plans, from TSOs and the EU DSO entity and determine a deadline for the submission of those proposals. TSOs, in cooperation with the EU DSO entity, may propose amendments to the competent authorities also on its own initiative. The proposals for amendment to the terms and conditions or methodologies, or for the amendments to the plans, shall be developed and approved in accordance with the procedure set out in this Article.

11. At least every three years after the first adoption of the respective terms and conditions or methodologies, or the respective adopted plans, TSOs in cooperation with the EU DSO entity, shall review the effectiveness of the adopted terms and conditions or methodologies, or the adopted plans, and shall report the findings of the review to the competent authorities and ACER without undue delay.

Article 9

Consultation

1. TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall consult stakeholders, including ACER, ENISA and the competent authority of each Member State, on the draft proposals for terms and conditions or methodologies listed in Article 6(2) and for plans referred to in Article 6(3). The consultation shall last for a period of not less than one month.

2. The proposals for terms and conditions or methodologies listed in Article 6(2) submitted by the TSOs, in cooperation with the EU DSO entity, shall be published and submitted to consultation at Union level. The proposals for plans listed in Article 6(3) submitted by the relevant TSOs, in cooperation with the EU DSO entity, at regional level shall be submitted to consultation at least at regional level.

3. TSOs, with the assistance of the ENTSO for Electricity, and the EU DSO Entity responsible for the proposal for terms and conditions or methodologies or plans shall duly take into account the views of stakeholders resulting from the consultations undertaken in accordance with paragraph 1, 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 and published in a timely manner before or simultaneously with the proposal for terms and conditions or methodologies.

Article 10

Stakeholder involvement

ACER, in close cooperation with ENTSO for Electricity and the EU DSO entity, shall organise stakeholder involvement, including regular meetings with stakeholders to identify problems and propose improvements related to the implementation of this Regulation.

Article 11

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, including the costs borne by the ENTSO for Electricity and the EU DSO entity, shall be assessed by the relevant NRA of each Member State.

2. Costs assessed as reasonable, efficient and proportionate shall be recovered through network tariffs or other appropriate mechanisms, as determined by the relevant NRA.

3. If requested by the relevant NRAs, TSOs and DSOs referred to in paragraph 1 shall, within a reasonable period determined by the NRA, provide the information necessary to facilitate the assessment of the costs incurred.

Article 12

Monitoring

1. ACER shall monitor the implementation of this Regulation in accordance with Article 32(1) of Regulation (EU) 2019/943 and Article 4(2) of Regulation (EU) 2019/942. In carrying out this monitoring, ACER may cooperate with ENISA and request support from the ENTSO for Electricity and the EU DSO entity. ACER shall regularly inform the Electricity Coordination Group and the NIS Cooperation Group on the implementation of this Regulation.

2. ACER shall publish a report at least every three years after the entry into force of this Regulation to

   (a) review the status of implementation of the applicable cybersecurity risk management measures with regard to the high-impact and critical-impact entities;

   (b) identify whether additional rules on common requirements, planning, monitoring, reporting and crisis management may be necessary to prevent risks for the electricity sector; and

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

3. By [*OP: please insert the date = 12 months after entry into force of this Regulation*], ACER, in cooperation with ENISA and after consultation of the ENTSO for Electricity and the EU DSO entity, may issue guidance on the relevant information to be communicated to ACER for the monitoring purposes as well as the process and

frequency for the collection, based on the performance indicators defined in accordance with paragraph 5.

4. The competent authorities may have access to the relevant information held by ACER, which it has collected in accordance with this Article.

5. ACER in cooperation with ENISA and with the support of the ENTSO for Electricity and the EU DSO entity, shall issue non-binding performance indicators for the assessment of operational reliability that are 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 for ACER to perform the tasks listed in paragraph 2.

Article 13

Benchmarking

1. By [*OP: please insert the date = within 12 months after the entry into force of this Regulation*], ACER, in cooperation with ENISA, shall establish a non-binding cybersecurity benchmarking guide. The guide shall explain to NRAs the principles of benchmarking of the implemented cybersecurity controls pursuant to paragraph 2 of this Article, taking into consideration the costs of implementing the controls and the effectiveness of the function played by processes, products, services, systems and solutions used to implement such controls. 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 for information.

2. Within 12 months after the establishment of the benchmarking guide pursuant to paragraph 1, the NRAs shall carry out a benchmarking analysis to assess whether current investments in cybersecurity:

   (a) mitigate risks having an impact on cross-border electricity flows;

   (b) provide the desired results and engender efficiency gains for the development of the electricity systems;

   (c) are efficient and integrated into the overall procurement of assets and services.

3. For the benchmarking analysis, the NRAs may take into account the non-binding cybersecurity benchmarking guide established by ACER, and shall assess in particular:

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

   (b) in cooperation with the ENTSO for Electricity and the EU DSO entity, the average prices of cybersecurity services, systems and products that contribute to a large extent to the enhancement and maintenance of the cybersecurity risk-management measures in the different system operation regions;

   (c) the existence and level of comparability of costs and functions of cybersecurity services, systems and solutions suitable for the implementation of this Regulation, identifying possible measures necessary to foster efficiency in

spending, particularly where cybersecurity technological investments may be needed.

4. Any information related to benchmarking analysis shall be handled 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 analysis referred to in paragraphs 2 and 3 shall not be made public.

5. Without prejudice to the confidentiality requirements in Article 47 and to the need to protect the security of entities subject to the provisions of this Regulation, the benchmarking analysis referred in paragraphs 2 and 3 of this Article shall be shared with all NRAs, all competent authorities, ACER, ENISA and the Commission.

Article 14

Agreements with TSOs from outside the Union

1. Within 18 months after the entry into force of this Regulation, TSOs of a system operation region that is neighbouring to a third country shall endeavour to conclude agreements with TSOs of the neighbouring third country that are in accordance with relevant Union law and that set out the basis for cooperation on cybersecurity protection and the cybersecurity cooperation arrangements with those TSOs.

2. TSOs shall inform the competent authority of the agreements concluded pursuant to paragraph 1.

Article 15

Legal representatives

1. Entities who do not have an establishment in the Union, but who deliver services to entities in the Union and have been notified as being high-impact or critical-impact entities in accordance with Article 24(6), shall, within three months after the notification, designate, in writing, a representative in the Union and inform the notifying competent authority accordingly.

2. This representative shall be mandated for the purpose of being addressed by any competent authority or a CSIRT in the Union in addition to or instead of the high-impact or critical-impact entity with regard to the obligations of the entity under this Regulation. The high-impact or critical-impact entity shall provide their legal representative with the necessary powers and sufficient resources to guarantee their efficient and timely cooperation with the relevant competent authorities or CSIRTs.

3. The representative shall be established in one of the Member States where the entity offers its services. The entity shall be deemed to be under the jurisdiction of the Member State where the representative is established. High-impact or critical-impact entities shall notify the name, postal address, email address and telephone number of their legal representative to the competent authority in the Member State where that legal representative resides or is established.

4. It shall be possible for the designated legal representative to be held liable for non-compliance with obligations under this Regulation, without prejudice to the liability

and legal actions that could be initiated against the high-impact or critical-impact entity itself.

5. In the absence of a representative within the Union designated under this Article, any Member State in which the entity provides services may take legal action against the entity for non-compliance with the obligations under this Regulation.

6. The designation of a legal representative within the Union pursuant to paragraph 1 shall not constitute an establishment in the Union.

Article 16

Cooperation between the ENTSO for Electricity and the EU DSO Entity

1. The ENTSO for Electricity and the EU DSO entity shall cooperate in performing cybersecurity risk assessments pursuant to Article 19 and Article 21, and in particular the following tasks:

   (a) development of the cybersecurity risk assessment methodologies pursuant to Article 18(1);

   (b) development of the Comprehensive Cross-border electricity cybersecurity risk assessment report pursuant to Article 23;

   (c) development of the common electricity cybersecurity framework pursuant to Chapter III;

   (d) development of the cybersecurity procurement recommendation pursuant to Article 35;

   (e) development of the cyber-attacks classification scale methodology pursuant to Article 37(8);

   (f) development of the provisional electricity cybersecurity impact index ('ECII') electricity cybersecurity impact index pursuant to Article 48(1) point (a);

   (g) development of the consolidated provisional list of high-impact and critical-impact entities pursuant to Article 48(3);

   (h) development of the provisional list of Union-wide high-impact and critical-impact processes pursuant to Article 48(4);

   (i) development of the provisional list of European and international standards and controls pursuant to Article 48(6);

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

   (k) performance of the regional cybersecurity risk assessments pursuant to Article 21;

   (l) definition of the regional cybersecurity risk mitigation plans pursuant to Article 22;

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

   (n) development of guidelines for the implementation of this Regulation in consultation with ACER and ENISA.

2. The cooperation between the ENTSO for Electricity and the EU DSO entity may take the form of a cybersecurity risk working group.

3. The ENTSO for Electricity and the EU DSO entity shall regularly inform ACER, ENISA, the NIS Cooperation Group and the Electricity Coordination Group on the progress in implementing the Union-wide and regional cybersecurity risk assessments pursuant Article 19 and Article 21.

Article 17

Cooperation between ACER and the competent authorities

ACER, in cooperation with each competent authority, shall:

(1) monitor the implementation of cybersecurity risk management measures pursuant to Article 12(2) point (a) and reporting obligations pursuant to Article 27 and Article 39; and

(2) monitor the adoption process and the implementation of the terms and conditions, methodologies or plans pursuant to Article 6(2) and (3). The cooperation between ACER, ENISA and each competent authority may take the form of a cybersecurity risk monitoring body.

CHAPTER II

RISK ASSESSMENT AND IDENTIFICATION OF THE RELEVANT CYBERSECURITY RISKS

Article 18

Cybersecurity risk assessment methodologies

1. By [*OP: please insert the date = within nine months after the entry into force of this Regulation*], the TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and following a consultation with the NIS Cooperation Group, shall submit a proposal for the cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level.

2. The cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level shall include:

   (a) 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;

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

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

(c) an approach to analyse the cybersecurity risks coming from legacy systems, the cascading effects of cyber-attacks and the real-time nature of systems operating the grid;

(d) an approach to analyse the cybersecurity risks coming from the dependency on a single supplier of ICT products, ICT services or ICT processes.

3. The cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level shall assess cybersecurity risks using the same risk impact matrix. The risk impact matrix shall:

(a) measure the consequences of cyber-attacks based on the following criteria:

(i) loss of load;

(ii) reduction of power generation;

(iii) loss of capacity in the primary frequency reserve;

(iv) loss of capacity for restoration of an electric grid to operation without relying on the external transmission network to recover after a total or partial shutdown (also called 'black start');

(v) the expected duration of an electricity outage affecting customers in combination with the scale of the outage in customer numbers; and

(vi) any other quantitative or qualitative criteria that could reasonably act as an indicator of the effect of a cyber-attack on cross-border electricity flows.

(b) measure the likelihood of an incident as the frequency of cyber-attacks per year.

4. The cybersecurity risk assessment methodologies at Union level shall describe how the ECII values for high-impact and critical-impact thresholds will be defined. The ECII shall enable entities to estimate with the help of the criteria referred to in paragraph 2 point (b), the impact of the risks on their business process during the business impact assessments they perform pursuant to Article 26(4) point (c)(i).

5. 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 paragraph 1.

Article 19

Union-wide cybersecurity risk assessment

1. Within 9 months after the approval of the cybersecurity risk assessment methodologies pursuant to Article 8 and every three years thereafter, the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group, shall, without prejudice to Article 22 of Directive (EU) 2022/2555, perform a Union-wide cybersecurity risk assessment and draw up a draft Union-wide cybersecurity risk assessment report. For this purpose, they will use the methodologies developed pursuant to Article 18, and approved pursuant to Article 8, 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 cybersecurity risk assessment shall not consider the legal, financial or reputational damage of cyber-attacks.

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

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

   (b) a risk impact matrix that entities and the competent authorities shall use to assess the cybersecurity risk identified in the cybersecurity risk assessment at Member State level performed pursuant to Article 20 and in the cybersecurity risk assessment at entity level pursuant to Article 26(2) point (b).

3. With respect to the Union-wide high-impact processes and the Union-wide critical-impact processes, the Union-wide cybersecurity risk assessment report shall include:

   (a) an assessment of the possible consequences of a cyber-attack using the metrics defined in the cybersecurity risk assessment methodology developed pursuant to Article 18(2), (3) and (4), and approved pursuant to Article 8;

   (b) the ECII and high-impact and critical-impact thresholds that the competent authorities shall use pursuant to Article 24(1) and (2) to identify high-impact and critical-impact entities involved in the Union-wide high-impact processes and in the Union-wide critical-impact processes.

4. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall submit the draft of the Union-wide cybersecurity risk assessment report with the results of the Union-wide cybersecurity risk assessment to ACER for opinion. ACER shall issue an opinion on the draft report within three months after its receipt. The ENTSO for Electricity and the EU DSO entity shall take utmost account of ACER's opinion when finalising that report.

5. Within three months after receipt of ACER's opinion, the ENTSO for Electricity, in cooperation with the EU DSO entity shall notify the final Union-wide cybersecurity risk assessment report to ACER, the Commission, ENISA and the competent authorities.

Article 20

Member State cybersecurity risk assessment

1. Each competent authority shall perform a Member State cybersecurity risk assessment on all high-impact and critical-impact entities in its Member State using the methodologies developed pursuant to Article 18 and approved pursuant to Article 8. The Member State cybersecurity risk assessment shall identify and analyse the risks of cyber-attacks affecting the operational security of the electricity system 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 notification of the high-and critical-impact entities pursuant to Article 24(6) and every three years after that date, and after consulting the CS-NCA responsible for electricity, each competent authority, 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 pursuant to Article 29;

(b) a list of all cyber-attacks reported in the previous three years pursuant to Article 38(3);

(c) a summary of the cyber threat information reported in the previous three years pursuant to Article 38(6);

(d) for each Union-wide high-impact or critical-impact process, an estimate of the risks of a compromise of the confidentiality, integrity and availability for information and relevant assets;

(e) where necessary, a list of additional entities identified as high-impact or critical-impact pursuant to Article 24(1), (2), (3), and (5).

3. The Member State cybersecurity risk assessment report shall take into account the Member State's risk preparedness plan established pursuant to Article 10 of Regulation (EU) 2019/941.

4. The information contained in the Member State cybersecurity risk assessment report pursuant to paragraph 2 points (a) to (d) shall not be linked to specific entities or assets. The Member State cybersecurity risk assessment report shall also include a risk assessment of the temporary derogations issued by the competent authorities in the Member States pursuant to Article 30.

5. The ENTSO for Electricity and the EU DSO entity may request additional information from the competent authorities in relation to the tasks specified in subparagraph 2 points (a) and (c).

6. The competent authorities shall ensure that the information they provide is accurate and correct.

Article 21

Regional cybersecurity risk assessments

1. The ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the relevant Regional Coordination Centre, shall perform a regional cybersecurity risk assessment for each system operation region using the methodologies developed pursuant to Article 19, and approved pursuant to Article 8, to 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. Within 30 months after the notification of the high-impact and critical-impact entities pursuant to Article 24(6), and every three years after that, the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group, shall draw up a regional cybersecurity risk assessment report for each system operation region.

3. The regional cybersecurity risk assessment report shall take into account the relevant information contained in the Union-wide cybersecurity risk assessment reports and in the Member State cybersecurity risk assessments reports.

4. The regional cybersecurity risk assessment shall consider the regional electricity crisis scenarios related to cybersecurity identified pursuant to Article 6 of the Regulation (EU) 2019/941.

Article 22

Regional cybersecurity risk mitigation plans

1. Within 36 months after the notification of the high-and critical-impact entities pursuant to Article 24(6) and no later than [*OP: please insert the date = 84 months after entry into force*], and every three years after that date, the TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the Regional Coordination Centres and the NIS Cooperation Group, shall develop a regional cybersecurity risk mitigation plan for each system operation region.

2. The regional cybersecurity risk mitigation plans shall include:

   (a) the minimum and advanced cybersecurity controls that high-impact and critical-impact entities shall apply in the system operation region;

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

3. The ENTSO for Electricity shall submit the regional risk mitigation plans to the relevant transmission system operators, to the competent authorities, and to the Electricity Coordination Group. The Electricity Coordination Group may recommend amendments.

4. The TSOs, with the assistance of the ENTSO for Electricity in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group shall update the regional risk mitigation plans every three years, unless circumstances warrant more frequent updates.

Article 23

Comprehensive cross-border electricity cybersecurity risk assessment report

1. Within 40 months after the notification of the high-and critical-impact entities pursuant to Article 24(6) and every three years thereafter, TSOs, with the assistance of the ENTSO for Electricity, in cooperation with the EU DSO entity and in consultation with the NIS Cooperation Group, shall provide to the Electricity Coordination Group a report on the outcome of the assessment of cybersecurity risks with regard to cross-border electricity flows (the 'comprehensive cross-border electricity cybersecurity risk assessment report').

2. The comprehensive cross-border electricity cybersecurity risk assessment report shall be based on the Union-wide cybersecurity risk assessment report, on the Member State cybersecurity risk assessment reports and on the regional cybersecurity risk assessment reports and include the following information:

(a) the list of Union-wide high-impact and critical-impact processes identified in the Union-wide cybersecurity risk assessment report in accordance with Article 19(2) point (a) including the estimation of likelihood and impact of cybersecurity risks evaluated during the regional cybersecurity risk assessment reports pursuant Article 21(2) and Article 19(3) point (a);

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

(c) cyber-attacks for the previous period at Union level, providing a critical overview of how such cyber-attacks 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 information flows pursuant to Articles 37 and 38;

(f) list of information or specific criteria for classification of information pursuant to Article 46;

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

(h) results and accumulated experiences from regional and cross-regional cybersecurity exercises organised pursuant to Article 44;

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

(j) any other information that may be useful to identify possible improvements of this Regulation or the need for a revision of this Regulation or any of its tools; and

(k) aggregated and anonymised information of derogations granted pursuant to Article 30(3).

3. The entities listed in Article 2(1) may contribute to the development of the comprehensive cross-border electricity cybersecurity risk assessment report, respecting the confidentiality of information in accordance with Article 47. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall consult these entities from an early stage.

4. The comprehensive cross-border electricity cybersecurity risk assessment report shall be subject to the rules on protection of exchange of information pursuant to Article 46. Without prejudice to Article 10(4) and Article 47(4), the ENTSO for Electricity and the EU DSO entity shall release a public version of that report which shall not contain information that can cause damage to entities listed in Article 2(1). The public version of this report shall only be released with the agreement of the NIS Cooperation Group and the Electricity Coordination Group. The ENTSO for Electricity in coordination with the EU DSO entity shall be responsible for the compilation and the release of the public version of the report.

Article 24

Identification of high-impact and critical-impact entities

1. Each competent authority shall identify, by using the ECII and high-impact and critical-impact thresholds included in the Union-wide cybersecurity risk assessment report pursuant to Article 19(3), point (b), the high-impact and critical-impact entities in its Member State that are involved in the Union-wide high-impact and critical-impact processes. The competent authorities can request information from an entity in their Member State to determine the ECII values for that entity. If the determined ECII of an entity is above the high-impact or critical-impact threshold, the identified entity shall be listed in the Member State cybersecurity risk assessment report referred to in Article 20(2).

2. Each competent authority shall identify, by using the ECII and high-impact and critical-impact thresholds included in the Union-wide cybersecurity risk assessment report pursuant to Article 19(3), point (b), the high-impact and critical-impact entities not established in the Union in so far they are active within the Union. The competent authority may request information from an entity not established in the Union to determine the ECII values for the entity.

3. Each competent authority may identify additional entities in its Member State as high-impact or critical-impact entities if the following 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;

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

4. If a competent authority identifies additional entities in accordance with paragraph 3, 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, and all processes at these entities for which the ECII aggregated over the group are above the critical-impact thresholds shall be considered critical-impact processes.

5. If a competent authority identifies entities referred to in paragraph 3 point (a) in more than one Member State, it shall inform the other competent authorities, the ENTSO for Electricity and the EU DSO entity. The ENTSO for Electricity in cooperation with the EU DSO entity, based on the information received from all competent authorities, shall provide to the competent authorities an analysis of the aggregation of entities in more than one Member State that can create a distributed disturbance to the cross-border electricity flows, and can result in a cyber-attack. Where a group of entities in several Member States is identified as an aggregation whose ECII is above the high-impact or critical-impact threshold, all concerned competent authorities shall identify the entities in such group as high-impact or critical-impact entities for their respective Member State, based on the aggregated ECII for the group of the entities, and the identified entities shall be listed in the Union-wide cybersecurity risk assessment report.

6. Each competent authority shall, within nine months after being notified by ENTSO for Electricity and EU DSO entity of the Union-wide cybersecurity risk assessment report pursuant to Article 19(5) and in any case no later than [*OP: please insert the date = 48 months after entry into force*], notify to the entities on the list that they have been identified as a high-impact or critical-impact entity in its Member State.

7. When a service provider is reported to a competent authority as being a critical ICT service provider pursuant Article 27 point (c), that competent authority shall notify it to the competent authorities of the Member States in whose territories the seat or representative is situated. The latter competent authority shall notify the service provider that it has been identified as being a critical service provider.

Article 25

National verification schemes

1. The competent authorities may establish a national verification scheme to verify that critical-impact entities identified pursuant to Article 24(1) have implemented the national legislative framework that is included in the mapping matrix referred to in Article 34. The national verification scheme may be based on an inspection carried out by the competent authority, independent security audits, or on mutual peer reviews by critical-impact entities in the same Member State supervised by the competent authority.

2. If a competent authority decides to establish a national verification scheme, that competent authority shall ensure that the verification is performed in accordance with the following requirements:

   (a) any party performing the peer review, audit 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, audit 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 and regulatory framework and European and international standards in scope of the verification;

      (vii) the critical-impact processes in scope of the verification.

   (c) the party performing the peer review, audit or inspection shall be allowed sufficient time to perform these activities;

   (d) the party performing the peer review, audit or inspection shall take the appropriate measures to protect the information they collect during the verification, in line with its confidentiality level; and

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

3. If a competent authority decides to establish a national verification scheme, it shall report to ACER on an annual basis how frequently it has carried out inspections under that scheme.

Article 26

Cybersecurity risk management at entity level

1. Each high-impact and critical-impact entity as identified by the competent authorities pursuant to Article 24(1) shall perform cybersecurity risk management for all its assets in its high-impact and critical-impact perimeters. Each high-impact and critical-impact entity shall perform risk management containing the phases in paragraph 2 every three years.

2. Each high-impact and critical-impact entity shall base its cybersecurity risk management on an approach that aims to protect their network and information systems and that comprises the following phases:

   (a) context establishment;

   (b) cybersecurity risk assessment at entity level;

   (c) cybersecurity risk treatment;

   (d) cybersecurity 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 the high-impact and critical-impact processes identified by the ENTSO for Electricity and the EU DSO entity, and other processes that may be targets of cyber-attacks with a high-impact or critical-impact on cross-border electricity flows; and

   (b) define the criteria for risk evaluation and for risk acceptance in accordance with the risk impact matrix that entities and the competent authorities shall use to assess the cybersecurity risks in the cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level developed by the ENTSO for Electricity and the EU DSO entity in accordance with Article 19(2).

4. During the cybersecurity risk assessment phase, each high-impact and critical-impact entity shall:

   (a) identify cybersecurity 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 Comprehensive cross-border electricity cybersecurity risk assessment report referred to in Article 23 and supply chain threats;

      (iii) vulnerabilities, including vulnerabilities in legacy systems;

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

      (v) relevant risk evaluations and assessments carried out at Union level, including coordinated risk assessments of critical supply chains in accordance with Article 22 of Directive (EU) 2022/2555, and

(vi) existing implemented controls.

(b) analyse the likelihood and consequences of the cybersecurity risks identified in point (a) and determine the cybersecurity risk level using the risk impact matrix used to assess cybersecurity risks in cybersecurity risk assessment methodologies at Union level, at regional level and at Member State level developed by TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity in accordance with Article 19(2);

(c) classify assets according to the possible consequences when cybersecurity is compromised and determine the high-impact and critical-impact perimeter using the following steps:

(i) perform, for all processes covered by the cybersecurity risk assessment, a business impact assessment using the ECII;

(ii) classify a process as high-impact or critical-impact if its ECII is above the high-impact or critical-impact threshold respectively;

(iii) determine all high-impact and critical-impact assets as the assets needed for the high-impact and critical-impact processes respectively;

(iv) define the high-impact and critical-impact perimeters containing all high-impact and critical-impact assets respectively, so that access to the perimeters may be controlled.

(d) evaluate cybersecurity risks by prioritizing them through risk evaluation criteria and risk acceptance criteria referred to in paragraph 3 point (b).

5. During the cybersecurity risk treatment phase, each high-impact and critical-impact entity shall establish an entity-level risk mitigation plan by selecting risk treatment options appropriate to manage the risks and identify the residual risks.

6. During the cybersecurity 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 point (b).

7. Each high-impact and critical-impact entity shall register the assets identified in paragraph 1 in an asset inventory. That asset inventory shall not be part of the risk assessment report.

8. The competent authority may inspect the assets in the inventory during inspections.

Article 27

Reporting on the risk assessment at entity level

Each high-impact and critical-impact entity shall, within 12 months after the notification of the high-and critical-impact entities pursuant to Article 24(6), and every three years thereafter, provide to the competent authority a report containing the following information:

(1) a list of controls selected for the entity-level risk mitigation plan pursuant to Article 26(5) with the current implementation status of each control;

(2) for each Union-wide high-impact or critical-impact process, an estimate of the risk of a compromise of the confidentiality, integrity, and availability of information and relevant assets. The estimate of this risk shall be given in accordance with the risk impact matrix in Article 19(2);

(3) a list of critical ICT service providers for their critical-impact processes.

CHAPTER III

COMMON ELECTRICITY CYBERSECURITY FRAMEWORK

Article 28

Composition, functioning and review of the common electricity cybersecurity framework

1. The common electricity cybersecurity framework shall be composed of the following controls and cybersecurity management system:
   (a) the minimum cybersecurity controls, developed in accordance with Article 29;
   (b) the advanced cybersecurity controls, developed in accordance with Article 29;
   (c) the mapping matrix, developed in accordance with Article 34, that maps the controls referred to in points (a) and (b) against selected European and international standards and national legislative or regulatory frameworks;
   (d) the cybersecurity management system established pursuant to Article 32.
2. All high-impact entities shall apply the minimum cybersecurity controls pursuant to paragraph 1 point (a) within their high-impact perimeter.
3. All critical-impact entities shall apply the advanced cybersecurity controls pursuant to paragraph 1 point (b) within their critical-impact perimeter.
4. Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant Article 19(4), the common electricity cybersecurity framework referred to in paragraph 1 shall be supplemented by the minimum and advanced cybersecurity controls in the supply chain developed pursuant to Article 33.

Article 29

Minimum and advanced cybersecurity controls

1. Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant Article 19(4), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity, shall develop a proposal for minimum and advanced cybersecurity controls.
2. Within 6 months after drawing up each regional cybersecurity risk assessment report pursuant Article 21(2) the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity, shall propose an amendment to the competent authority for the minimum and advanced cybersecurity controls. The proposal will be done in accordance with Article 8(10) and will take into account the risks identified in the regional risk assessment.
3. The minimum and advanced cybersecurity controls shall be verifiable by taking part in a national verification scheme in accordance with the procedure set out in Article 31 or by undergoing independent third-party security audits performed according to the requirements listed in Article 25(2).

4. The initial minimum and advanced cybersecurity controls developed pursuant to paragraph (1) shall be based on the risks that are identified in the Union-wide cybersecurity risk assessment report referred to in Article 19(5). The amended minimum and advanced cybersecurity controls developed pursuant to paragraph (2) shall be based on the regional cybersecurity risk assessment report referred to in Article 21(2).

5. The minimum cybersecurity controls shall include controls to protect the information exchanged pursuant to Article 46.

6. Within 12 months after the approval of the minimum and advanced cybersecurity controls pursuant to Article 8(5), or after each update pursuant to Article 8(10), the entities listed in Article 2(1) and identified as critical-impact and high-impact entities pursuant to Article 24 shall, during the establishment of the entity-level risk mitigation plan pursuant to Article 26(5), apply the minimum cybersecurity controls within the high-impact perimeter and advanced cybersecurity controls within the critical-impact perimeter.

Article 30

Derogations from the minimum and advanced cybersecurity controls

1. The entities listed in Article 2(1) may request the respective competent authority to grant a derogation from their obligation to apply the minimum and advanced cybersecurity controls referred to in Article 29(6). The competent authority may grant such a derogation on one of the following grounds:

   (a) in exceptional circumstances, where the entity can demonstrate that the costs of implementing the appropriate cybersecurity controls significantly exceed the benefits. ACER and the ENTSO for Electricity in cooperation with the DSO entity may jointly develop a guidance for estimating the costs of cybersecurity controls to help the entities;

   (b) where the entity provides an entity-level risk treatment plan that mitigates the cybersecurity risks using alternative controls to a level that is acceptable in accordance with to the risk acceptance criteria referred to Article 26(3), point (b).

2. Within three months from the receipt of the request referred to in paragraph 1, each competent authority shall decide whether a derogation from the minimum and advanced cybersecurity controls is to be granted. Derogations from the minimum or advanced cybersecurity controls shall be granted for a maximum of three years, with the possibility of renewal.

3. Aggregated and anonymised information for the derogations granted shall be included as an annex to the comprehensive cross-border electricity cybersecurity risk assessment report referred to in Article 23. The ENTSO for Electricity and the EU DSO entity shall jointly update the list, where necessary.

Article 31

Verification of the common electricity cybersecurity framework

1. No later than 24 months after the adoption of the controls referred to in points (a), (b) and (c) of Article 28(1) and the establishment of the cybersecurity management system referred to in point (d) of that Article, each critical-impact entity identified in accordance with Article 24(1) shall be able to demonstrate its compliance with the cybersecurity management system and the minimum or advanced cybersecurity controls at the request of the competent authority.

2. Each critical-impact entity shall fulfil the obligation referred to in paragraph 1 by undergoing independent third-party security audits in accordance with the requirements listed in Article 25(2) or by taking part in a national verification scheme in accordance with Article 25(1).

3. The verification that a critical-impact entity complies with the cybersecurity management system and the minimum or advanced cybersecurity controls shall cover all assets within the critical-impact perimeter of the critical-impact entity.

4. The verification that a critical-impact entity complies with the cybersecurity management system and the minimum or advanced cybersecurity controls shall be regularly repeated at the latest 36 months after the end of the first verification, and every 3 years thereafter.

5. Each critical-impact entity defined in accordance with Article 24 shall demonstrate its compliance with the controls referred to in points (a), (b) and (c) of Article 28(1) and the establishment of the cybersecurity management system referred to in point (d) of that Article by reporting on the outcome of the compliance verification to the competent authority.

Article 32

Cybersecurity management system

1. Within 24 months after being notified by the competent authority that they have been identified as a high-impact or critical-impact entity in accordance with Article 24(6), each high-impact and critical-impact entity shall establish a cybersecurity management system, and review it every three years thereafter, to:

   (a) determine the scope of the cybersecurity management system considering interfaces and dependencies with other entities;

   (b) ensure that all its senior management is informed of relevant legal obligations and actively contributes to the implementation of the cybersecurity management system through timely decisions and prompt reactions;

   (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 at entity level as defined in Article 26;

(g) determine and provide the resources required for the implementation, maintenance and continual improvement of the cybersecurity management system, taking into account the necessary competence and awareness of cybersecurity resources;

(h) determine the internal and external communication that is relevant to cybersecurity;

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

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

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

(l) review the implementation of the cybersecurity management system at planned intervals; and control and correct non-compliance of the resources and activities with the policies, procedures, guidelines in the cybersecurity management system.

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

3. The competent authorities shall, without imposing or discriminating in favour of the use of a particular type of technology, encourage the use of European or international standards and specifications related to management systems and relevant to the security of network and information systems.

Article 33

Minimum and advanced cybersecurity controls in the supply chain

1. Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant Article 19(4), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall develop a proposal for minimum and advanced cybersecurity controls in the supply chain that mitigate the supply chain risks identified in the Union-wide cybersecurity risk assessments, supplementing the minimum and advanced cybersecurity controls developed pursuant to Article 29. The minimum and advanced cybersecurity controls in the supply chain shall be developed together with the minimum and advanced cybersecurity controls pursuant to Article 29. The minimum and advanced cybersecurity controls in the supply chain shall cover the entire lifecycle of all ICT products, ICT services and ICT processes inside the high-impact or critical-impact perimeters of a high-impact or critical-impact entity. The NIS Cooperation Group shall be consulted when developing the proposal for minimum and advanced cybersecurity controls in the supply chain.

2. The minimum cybersecurity controls in the supply chain shall consist of controls for high-impact and critical-impact entities that:

(a) include recommendations for the procurement of ICT products, ICT services, and ICT processes referring to cybersecurity specifications, covering at least:

(i) the 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. Background verification check may include a verification of the identity and background of staff or contractors of an entity in accordance with national law and procedures and relevant and applicable Union law, including Regulation (EU) 2016/679 and Directive (EU) 2016/680 of the European Parliament and of the Council[24]. Background checks shall be proportionate and strictly limited to what is necessary. They shall be carried out for the sole purpose of evaluating a potential security risk to the entity concerned. They need to be proportional to business requirements, the classification of the information to be accessed and the perceived risks, and may be performed by the entity itself, by an external company performing a screening, or through a government clearing;

(ii) the processes for secure and controlled design, development and production of ICT products, ICT services and ICT processes, promoting the design and development of ICT products, ICT services, and ICT processes, which include appropriate technical measures to ensure cybersecurity;

(iii) design of network and information systems in which devices are not trusted even when they are within a secure perimeter, require verification of all requests they receive and apply the least privilege principle;

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

(v) the contractual obligations on the supplier to protect and restrict access to the entity's sensitive information;

(vi) the underpinning cybersecurity procurement specifications to subcontractors of the supplier;

(vii) the traceability of the application of the cybersecurity specifications from the development through production until delivery of ICT products, ICT services or ICT processes;

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

(ix) the right to audit cybersecurity in the design, development and production processes of the supplier; and

(x) The assessment of the risk profile of the supplier.

(b) require such entities to take into account the procurement recommendations referred to in subparagraph (a) when concluding 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

[24] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ L 119, 4.5.2016, p. 89)

unsolicited events and circumstances like termination and transition of contracts in cases of negligence of the contractual partner;

(c) require such entities to take into account the results of relevant coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1) of Directive (EU) 2022/2555;

(d) include criteria to select and contract suppliers that can meet the cybersecurity specifications as stated in paragraph (a) 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;

(e) include criteria to diversify sources of supply for ICT products, ICT services and ICT processes and reduce the risk of a vender lock-in;

(f) include criteria to monitor, review or audit the cybersecurity specifications for supplier internal operational processes throughout the entire lifecycle of each ICT product, ICT service and ICT process on a regular basis.

3. For the cybersecurity specifications in the cybersecurity procurement recommendation referred to in paragraph 2 point (a), high-impact or critical-impact entities shall use the principles of procurement pursuant to Directive (EC) 2014/24, in accordance with Article 35(4), or define their own specifications based on the results of the cybersecurity risk assessment at entity level.

4. The advanced cybersecurity controls in the supply chain 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 specifications. The ICT product, ICT service or ICT process shall be verified either through a European cybersecurity certification scheme referred to in Article 31 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 controls in the supply chain shall apply to the procurement of relevant ICT product, ICT services and ICT processes. The minimum and advanced cybersecurity controls of the supply chain will apply to procurement processes in the entities identified as critical-impact and high-impact entities pursuant to Article 24 that starts six months after the adoption or update of the minimum and advanced cybersecurity controls referred to in Article 29.

6. Within 6 months after drawing up each regional cybersecurity risk assessment report pursuant Article 21(2) the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity, shall propose an amendment to the competent authority for the minimum and advanced cybersecurity controls in the supply chain. The proposal will be done in accordance with Article 8(10) and will take into account the risks identified in the regional risk assessment.

Article 34

Mapping matrix for electricity cybersecurity controls against standards

1. Within 7 months after submitting the first draft Union-wide cybersecurity risk assessment report pursuant Article 19(4), the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity and in consultation with ENISA, shall develop a proposal for a matrix to map the controls set out in Article 28(1) points (a) and (b) against selected European and international standards as well as relevant technical specifications ('the mapping matrix'). The ENTSO for Electricity and the EU DSO entity shall document the equivalence of the different controls with the controls set out in Article 28(1), points (a) and (b).

2. The competent authorities may provide to the ENTSO for Electricity and the EU DSO entity a mapping of the controls set out in Article 28(1), points (a) and (b) with a reference to the related national legislative or regulatory frameworks, including relevant national standards of Member States pursuant to Article 25 of Directive (EU) 2022/2555. If the competent authority of a Member State provides such a mapping, the ENTSO for Electricity and the EU DSO entity shall integrate this national mapping into the mapping-matrix.

3. Within 6 months after drawing up each regional cybersecurity risk assessment report pursuant Article 21(2) the TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO Entity and in consultation with ENISA, shall propose an amendment to the competent authority for mapping matrix. The proposal will be done in accordance with Article 8(10) and will take into account the risks identified in the regional risk assessment.

CHAPTER IV

CYBERSECURITY PROCUREMENT RECOMMENDATIONS

Article 35

Cybersecurity procurement recommendations

1. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall develop, in a work programme to be established and updated each time a regional cybersecurity risk assessment report is adopted, sets of non-binding cybersecurity procurement recommendations that 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. This work programme shall include the following:

   (a) a description and classification of the types of ICT products, ICT services and ICT processes used by high-impact and critical-impact entities in the high-impact and critical-impact perimeter;

   (b) a list of the types of ICT products, ICT services, and ICT processes for which a set of non-binding cybersecurity recommendations shall be developed based on the relevant regional cybersecurity risk assessment reports and on the priorities of high-impact and critical-impact entities.

2. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall, within 6 months after the adoption or update of the regional cybersecurity risk assessment report provide ACER with a summary of that work programme.

3. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall endeavour to ensure that the non-binding cybersecurity procurement recommendations developed based on the relevant regional cybersecurity risk assessment are similar or comparable across system operation regions. The sets of cybersecurity procurement recommendations shall cover at least the specifications referred to in Article 33(2), point (a). Where possible, the specifications shall be selected from European and international standards.

4. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity, shall ensure that the sets of cybersecurity procurement recommendations:

   (a) comply with the principles of procurement pursuant to Directive (EC) 2014/24; and

   (b) are compatible with and take in account the most recent available European cybersecurity certification schemes relevant to the ICT product, ICT service, or ICT process.

Article 36

Guidance on use of European cybersecurity certification schemes for procurement of ICT products, ICT services and ICT processes

1. The non-binding cybersecurity procurement recommendations developed pursuant to Article 35 may include 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 used by critical-impact entities, without prejudice to the framework for the establishment of European cybersecurity certification schemes pursuant to Article 46 of Regulation (EU) 2019/881.

2. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall closely cooperate with ENISA in providing the sector-specific guidance included in non-binding cybersecurity procurement recommendations pursuant to paragraph 1.

CHAPTER V

INFORMATION FLOWS, CYBER-ATTACKS AND CRISIS MANAGEMENT

Article 37

Rules on information sharing

1. If a competent authority receives information related to a reportable cyber-attack, that competent authority:

   (a) shall assess the level of confidentiality of that information and inform the entity about the outcome of its assessment without undue delay and not later than within 24 hours of receipt of the information;

(b) shall attempt to find any other similar cyber-attack in the Union reported to other competent authorities, in order to correlate the information received in the context of the reportable cyber-attack with information provided in the context of other cyber-attacks and enrich existing information, strengthen and coordinate cybersecurity responses;

(c) shall be responsible for the removal of business secrets and the anonymisation of the information in accordance with the relevant national and Union rules;

(d) shall share the information with the national single points of contact, CSIRTs and all competent authorities designated pursuant to Article 4 in other Member States without undue delay and no later than 24 hours after the reception of a reportable cyber-attack and provide updated information on a regular basis to those authorities or bodies;

(e) shall disseminate the information of the cyber-attack, after anonymisation and removal of business secrets pursuant to paragraph 1(c), to critical-impact and high-impact entities in its Member State without undue delay and no later than 24 hours after receiving information according to paragraph 1(a), and provide updated information on a regular basis allowing the entities to organise their defence effectively;

(f) may request the reporting high-impact or critical-impact entity to further disseminate the reportable cyber-attack information in a secure manner to other entities that may be affected, with the aim to generate situational awareness by the electricity sector and to prevent the materialisation of a risk that may escalate in a cross-border cybersecurity electricity incident;

(g) shall share with ENISA a summary report, after anonymisation and removal of business secrets, with the information of the cyber-attack.

2. If a CSIRT becomes aware of an unpatched actively exploited vulnerability, it shall:

(a) share it with ENISA via an appropriate secure information exchange channel without delay, unless otherwise specified in other Union law;

(b) support the concerned entity to receive from the manufacturer or provider an effective, coordinated and rapid management of the unpatched actively exploited vulnerability or of effective and efficient mitigation measures;

(c) share available information with the vendor and request the manufacturer or provider, where possible, to identify a list of CSIRTs in Member States concerned by the unpatched actively exploited vulnerability and that shall be informed;

(d) share available information with the CSIRTs identified under the previous point, based on need-to-know principle;

(e) share, where they exist, mitigation strategies and measures to the reported unpatched actively exploited vulnerability.

3. If a competent authority becomes aware of an unpatched actively exploited vulnerability, that competent authority shall:

(a) share, where they exist, mitigation strategies and measures to the reported unpatched actively exploited vulnerability, in coordination with the CSIRTs in its Member State;

(b) shall share the information with a CSIRT in the Member State where the unpatched actively exploited vulnerability has been reported.

4. If the competent authority becomes aware of an unpatched vulnerability, without evidence of yet being actively exploited, it shall without undue delay coordinate with the CSIRT for the purposes of coordinated vulnerability disclosure as laid down in Article 12(1) of Directive (EU) 2022/2555.

5. If a CSIRT receives information related to cyber threats from one or several high-impact or critical-impact entities pursuant to Article 38(6), it shall disseminate that information or any other information of importance for preventing, detecting, responding to or mitigating the related risk to critical-impact and high-impact entities in its Member State and, where appropriate, to all concerned CSIRTs and to its national single point of contact without undue delay and no later than four hours after receiving information.

6. If a competent authority becomes aware of information related to cyber threats from one or several high-impact or critical-impact entities, it shall forward this information to the CSIRT for the purpose of paragraph 5.

7. The competent authorities may delegate in full or in part the responsibilities under paragraphs 3 and 4 concerning one or more high-impact or critical-impact entities that operate in more than one Member State to another competent authority in one of those Member States, following an agreement among the concerned competent authorities.

8. The TSOs, with the assistance of the ENTSO for Electricity, and in cooperation with the EU DSO entity shall develop a cyber-attack classification scale methodology by [*OP: please insert the date = within 12 months after the entry into force of this Regulation*]. The TSOs, with the assistance of the ENTSO for Electricity and the EU DSO entity may request the competent authorities to consult ENISA and their competent authorities responsible for cybersecurity for assistance in the development of such classification scale. The methodology shall provide the classification for the gravity of a cyber-attack according to 5 levels, the two highest levels being 'high' and 'critical'. The classification shall be based on the assessment of the following parameters:

(a) the potential impact considering the assets and perimeters exposed determined in accordance with Article 26(4), point (c); and

(b) the severity of the cyber-attack.

9. By [*OP: please insert the date = within two years after the entry into force of this Regulation*], the ENTSO for Electricity, in collaboration with the EU DSO entity, shall perform a feasibility study to assess the possibility and the financial costs necessary to develop a common tool enabling all entities to share information with relevant national authorities.

10. The feasibility study shall address the possibility for such a common tool to:

(a) 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 cyber-attacks, early alerts related to cybersecurity matters and undisclosed vulnerabilities on equipment in use in the electricity system;

(b) be maintained in a suitable and highly trustable environment;

(c) allow for data collection from critical-impact and high-impact entities and facilitate removal of confidential information and anonymisation of the data and their prompt dissemination to critical-impact and high-impact entities.

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

(a) consult ENISA and the NIS Cooperation Group, the national single points of contact and the representatives of main stakeholders when assessing the feasibility;

(b) present the results of the feasibility study to ACER and the NIS Cooperation Group.

12. The ENTSO for Electricity, in cooperation with the EU DSO entity may analyse and facilitate initiatives proposed by critical-impact and high-impact entities to evaluate and test such tools for information sharing.

Article 38

Role of high-impact and critical-impact entities as regards information sharing

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

(a) establish, for all assets within its cybersecurity perimeter determined pursuant to Article 26(4) point (c), at least the CSOC capabilities to:

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

(ii) conduct security monitoring, including detecting intrusions and assessing vulnerabilities of network and information systems;

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

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

(b) have the right to procure all or parts of these capabilities pursuant to point (a) through MSSPs. Critical-impact and high-impact entities shall remain responsible for MSSPs and supervise their efforts;

(c) designate a single point of contact at entity level for the purpose of information sharing.

2. ENISA may issue non-binding guidance on establishing such capabilities or subcontracting the service to MSSPs, as part of the task defined in Article 6(2) of Regulation (EU) 2019/881.

3. Each critical-impact and high-impact entity shall share relevant information related to a reportable cyber-attack with its CSIRTs and its competent authority without undue delay and no later than four hours of becoming aware that the incident is reportable.

4. Information related to a cyber-attack shall be considered reportable when the cyber-attack is assessed by the affected entity resulting in a criticality ranging from “high” to “critical” following the cyber-attack classification scale methodology pursuant to

Article 37(8). The single point of contact at entity level designated pursuant to paragraph 1 point (c) shall communicate the incident classification.

5. Where critical-impact and high-impact entities notify relevant information related to unpatched actively exploited vulnerabilities to a CSIRT, the latter may forward this information to its competent authority. In light of the level of sensitivity of the notified information, the CSIRT may withhold the information or delay its forwarding based on justified cybersecurity-related grounds.

6. Each critical-impact and high-impact entity shall provide without undue delay to its CSIRTs any information related to a reportable cyber threat that may have a cross-border effect. Information related to a cyber threat shall be considered reportable when at least one of the following conditions is met:

   (a) it provides relevant information for other critical-impact and high-impact entity for preventing, detecting, responding or mitigating the impact of the risk;

   (b) the identified techniques, tactics and procedures used in the context of an attack lead to information such as compromised URL or IP addresses, hashes or any other attribute useful to contextualise and correlate the attack;

   (c) a cyber threat may be further assessed and contextualised with additional information provided by service providers or third parties not subject to this Regulation.

7. Each critical-impact entity and high-impact entity shall, when sharing information pursuant to this Article, specify the following:

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

   (b) whether the information concerns:

      (i) a reportable cyber-attack referred to in paragraph 3;

      (ii) unpatched actively exploited vulnerabilities not publicly known referred to in paragraph 4;

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

   (c) in the case of a reportable cyber-attack, the level of the cyber-attack according to the cyber-attack classification scale methodology referred to in Article 37(8) and information leading to this classification including at least the criticality of the cyber-attack.

8. When a critical or high-impact entity notifies a significant incident pursuant to Article 23 of Directive (EU) 2022/2555 and the incident reporting under that Article contains relevant information as required under paragraph 3 of this Article, the reporting of the entity under Article 23(1) of that Directive shall constitute reporting of information under paragraph 3 of this Article.

9. Each critical-impact and high-impact entity shall report to its competent authority or CSIRT by clearly identifying specific information that shall only be shared with the competent authority or CSIRT in cases where the information sharing could be source of a cyber-attack. Each critical-impact and high-impact entity shall have the right to provide a non-confidential version of the information to the competent CSIRT.

Article 39

Detection of cyber-attacks and handling of related information

1. Critical-impact and high-impact entities shall develop the necessary capabilities to handle detected cyber-attacks with the necessary support from the relevant competent authority, the ENTSO for Electricity and the EU DSO entity. The critical-impact and high-impact entities may be supported by the CSIRT designated in their respective Member State as part of the task assigned to the CSIRTs by Article 11(5) point (a) of Directive (EU) 2022/2555. Critical-impact and high-impact entities shall implement effective processes to identify, classify and respond to cyber-attacks that will or may affect cross-border electricity flows in order to minimise their impact.

2. If a cyber-attack has an effect on cross-border electricity flows, the single points of contact at entity level of affected critical-impact and high-impact entities shall cooperate to share information among them, coordinated by the competent authority of the Member State in which the cyber-attack was first reported.

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

   (a) ensure that their own single point of contact at entity level has access on a need-to-know basis to the information they received from the national single point of contact through their competent authority;

   (b) unless already done pursuant to Article 3(4) of Directive (EU) 2022/2555, notify the competent authority of the Member State in which they are established and the national single point of contact with a list of their cybersecurity single points of contact at entity level:

      (i) from which that competent authority and national single point of contact may expect to receive information about reportable cyber-attacks;

      (ii) to which competent authorities and national single points of contact may have to provide information.

   (c) establish cyber-attack management procedures for cyber-attacks, including roles and responsibilities, tasks and reactions based on the observable evolution of the cyber-attack within the critical-impact and high-impact perimeters;

   (d) test the overall cyber-attack management procedures at least every year by testing at least one scenario affecting directly or indirectly cross-border electricity flows. That annual test may be conducted by critical-impact and high-impact entities during the regular exercises referred to in Article 43. Any live cyber-attack response activity with a consequence classified at least Scale 2, according to the cyber-attack classification scale methodology referred to in Article 37(8) and with a cybersecurity root cause, may serve as an annual test of the cyber-attack response plan.

4. The tasks referred to in paragraph 1 may be delegated by the Member States also to the Regional Coordination Centres in accordance with Article 37(2) of Regulation (EU) 2019/943.

Article 40

Crisis management

1. When the competent authority establishes that an electricity crisis is related to a cyber-attack which has an impact on more than one Member State, the competent authorities from the affected Member States, the CS-NCAs, the RP-NCA and the NIS cyber crisis management authorities from the affected Member States shall jointly create an ad-hoc cross-border crisis coordination group.

2. The ad hoc cross-border 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) organise the communication between all the entities impacted by the crisis and the competent authorities, in order to reduce overlaps and increase the efficiency in the analyses and technical responses to remedy the simultaneous electricity crises with a cybersecurity root cause;

   (c) provide, in cooperation with the competent CSIRTs, the expertise required, including operational advice on the implementation of possible mitigation measures to the entities impacted by the incident;

   (d) notify and provide regular updates on the state of the incident to the Commission and the Electricity Coordination Group, following the protection principles laid down in Article 46;

   (e) seek advice from relevant authorities, agencies or entities that might be of help to mitigate the electricity crisis.

3. Where the cyber-attack qualifies or is expected to qualify as a large-scale cybersecurity incident, the ad-hoc cross-border crisis coordination group shall immediately inform the national cyber crisis management authorities in accordance with Article 9(1) of Directive (EU) 2022/2555 in the Member States affected by the incident, as well as the Commission and the EU CyCLONe. In such situation, the ad-hoc cross-border crisis coordination group shall support the EU CyCLONe concerning sectoral specificities.

4. Critical-impact and high-impact entities shall develop and have at their disposal capabilities, internal guidelines, preparedness plans, and staff to take part in the detection and mitigation of cross-border crisis. The critical-impact or high-impact entity impacted by a simultaneous electricity crisis shall investigate the root cause of such crisis in cooperation with its competent authority to determine the extent to which the crisis is related to a cyber-attack.

5. The tasks in paragraph 4 may be delegated by the Member States also to the Regional Coordination Centres in accordance with Article 37(2) of Regulation (EU) 2019/943.

Article 41

Cybersecurity Crisis management and response plans

1. Within 24 months after the notification to ACER of the Union-wide risk assessment report, ACER shall in close cooperation with ENISA, the ENTSO for Electricity, the EU DSO entity, CS-NCAs, competent authorities, RP-NCAs, the NRAs and the NIS national cyber crisis management authorities, develop a Union-level cybersecurity crisis management and response plan for the electricity sector.

2. Within 12 months after the development by ACER of the Union-level cybersecurity crisis management and response plan for the electricity sector pursuant to paragraph 1, each competent authority shall develop a national cybersecurity crisis management and response plan for cross-border electricity flows taking into account the Union-level cybersecurity crisis management plan and the national risk preparedness plan established in accordance with Article 10 of Regulation (EU) 2019/941. This plan shall be consistent with the large-scale cybersecurity incident and crisis response plan pursuant to Article 9(4) of Directive (EU) 2022/2555. The competent authority shall coordinate with the critical-impact and high-impact entities and with the RP-NCA in its Member State.

3. The national large-scale cybersecurity incident and crisis response plan required pursuant to Article 9(4) of Directive (EU) 2022/2555 shall be considered as a national cybersecurity crisis management plan under this Article if it includes crisis management and response provisions for the cross-border electricity flows.

4. The tasks listed in at paragraphs 1 and 2 may be delegated by the Member States also to the Regional Coordination Centres in accordance with Article 37(2) of Regulation (EU) 2019/943.

5. Critical-impact and high-impact entities shall ensure that their cybersecurity-related crisis management processes:

   (a) have compatible cross-border cybersecurity incident handling procedures as defined in Article 6(8) of Directive (EU) 2022/2555 formally incorporated in their crisis management plans;

   (b) are part of the general crisis management activities.

6. Within 12 months after the notification of the high-and critical-impact entities pursuant to Article 24(6), and every three years thereafter, critical impact and high-impact entities shall develop a crisis management plan at entity level for a cybersecurity related crisis which shall be included into their general crisis management plans. This plan shall include at least the following:

   (a) rules of declaration of the crisis as set out 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 entities;

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

7. The measures for crisis management pursuant to Article 21(2) point (c) of Directive (EU) 2022/2555 shall be considered as a crisis management plan at entity level for

the electricity sector under this Article if it includes all requirements listed in paragraph 6.

8. The crisis management plans shall be tested during the cybersecurity exercises referred to in Articles 43, 44 and 45.

9. The critical-impact and high-impact entities shall include their crisis management plans at entity level into their business continuity plans for the critical-impact and high-impact 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;

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

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

11. ACER shall update the Union-level cybersecurity crisis management and response plan for the electricity sector developed pursuant to paragraph (1) at least every three years and whenever necessary.

12. Each competent authority shall update the national cybersecurity crisis management and response plan for cross-border electricity flows developed pursuant to paragraph (2) at least every three years and whenever necessary.

13. The critical-impact and high-impact entities shall test their business continuity plans at least once every three years or after major changes in a critical-impact 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.

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

15. If 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.

16. Where a critical-impact or high-impact entity cannot correct the deficiencies within 180 calendar days, it shall include the reasons in the report to be provided to its competent authority in accordance with Article 27.

Article 42

Cybersecurity early alert capabilities for the electricity sector

1. The competent authorities shall cooperate with ENISA to develop Electricity Cybersecurity Early Alert Capabilities (ECEAC) as part as the assistance to Member States pursuant to Articles 6(2) and (7) of Regulation (EU) 2019/881.

2. The ECEAC shall enable ENISA when carrying out the tasks listed in Article 7(7) of Regulation (EU) 2019/881 to:

(a) collect voluntary shared information from:

(i) CSIRTs, competent authorities;

(ii) the entities listed in Article 2 of this Regulation;

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

(b) assess and classify collected information;

(c) assess 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 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 on the identified risks and recommended preventive actions specific to the entities concerned;

(g) inform all relevant entities listed in Article 2 on the results of the information assessed in accordance with points (b), (c) and (d) of this paragraph;

(h) periodically include the relevant information in the situational awareness report, issued in accordance with Article 7(6) of Regulation(EU) 2019/881;

(i) derive, where possible, applicable data that indicates that a potential security breach or cyber-attack ('indicators of compromise') from the collected information.

3. The CSIRTs shall disseminate the information received from ENISA to the entities concerned without delay, within their tasks defined in Article 11(3) point (b) of Directive (EU) 2022/2555.

4. ACER shall monitor the effectiveness of the ECEAC. ENISA shall assist ACER by providing all necessary information, pursuant to Articles 6(2) and 7(1) of Regulation(EU) 2019/881. The analysis of this monitoring activity shall be part of the monitoring pursuant to Article 12 of this Regulation.

CHAPTER VI

ELECTRICITY CYBERSECURITY EXERCISE FRAMEWORK

Article 43

Cybersecurity exercises at entity and Member State levels

1. By 31/12 of the year after the notification of critical-impact entities, and every three years thereafter, each critical-impact entity shall perform a cybersecurity exercise including one or more scenarios with cyber-attacks affecting cross-border electricity flows directly or indirectly and related to the risks identified during the cybersecurity risk assessments at Member State and entity levels in accordance with Article 20 and Article 27.

2. By derogation from paragraph 1, the RP-NCA, after consulting the competent authority and the relevant cyber crisis management authority as designated or

established in Directive (EU) 2022/2555 under Article 9 may decide to organise a cybersecurity exercise at Member State level as described in paragraph 1 instead of performing the cybersecurity exercise at entity level. In this regard, the competent authority shall inform:

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

(b) each entity that shall participate in the cybersecurity exercise at Member State level at the latest 6 months before the exercise is to take place.

3. The RP-NCA with the technical support of its CSIRTs, shall organise the cybersecurity exercise described in paragraph 2 at Member State level independently or in the context of a different cybersecurity exercise in that Member State. In order to be able to group these exercises, RP-NCA may postpone the cybersecurity exercise at Member State level referred to in paragraph 1 by one year.

4. The cybersecurity exercises at entity level and at Member State level shall be consistent with the national cybersecurity crisis management frameworks in accordance with Article 9(4), point (d) of Directive (EU) 2022/2555.

5. By [*OP: please insert the date = 31 December of the second year following the entry into force of this Regulation*], and every three years thereafter, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall make available an exercise scenario template to perform the cybersecurity exercises at entity and Member State level referred to in paragraphs 1. This template shall take into account the results of the most recently performed cybersecurity risk assessment at entity and Member State levels and shall include key success criteria. The ENTSO for Electricity and the EU DSO entity shall involve ACER and ENISA in the development of such template.

Article 44

Regional or cross regional cybersecurity exercises

1. By [*OP: please insert the date = 31 December of the fifth year following the entry into force of this Regulation*], and every three years thereafter, in each system operation region, the ENTSO for Electricity, in cooperation with the EU DSO entity, shall organise a regional cybersecurity exercise. The critical-impact entities in the system operation region shall participate in the regional cybersecurity exercise. The ENTSO for Electricity, in cooperation with the EU DSO entity, may organise, instead of a regional cybersecurity exercise, a cross regional cybersecurity exercise in more than one system operating regions in the same timeframe. The exercise should take into account other existing cybersecurity risk assessments and scenarios developed at Union level.

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

3. The ENTSO for Electricity, in coordination with the EU DSO entity, shall inform the critical-impact entities that shall participate in the regional or cross regional cybersecurity exercise six months before the exercise takes place.

4. The organiser of a regular cybersecurity exercise at Union level pursuant Article 7(5) of Regulation (EU) 2019/881, or of any mandatory cybersecurity exercise related to the electricity sector within the same geographic perimeter, may invite the ENTSO for Electricity and the EU DSO entity to participate. In such cases, the obligation in paragraph 1 does not apply, provided that all critical-impact entities in the system operation region take part in the same exercise.

5. If the ENTSO for Electricity and the EU DSO entity participate in a cybersecurity exercise referred to in paragraph 4, they may postpone the regional or cross-regional cybersecurity exercise referred to in paragraph 1 by one year.

6. By [*OP: please insert the date = 31 December of the third year following the entry into force of this Regulation*], and every three years after that date, the ENTSO for Electricity, in coordination with the EU DSO entity, shall make available an exercise template to perform the regional and cross regional cybersecurity exercises. This template shall take into account the results of the most recently performed cybersecurity risk assessment at regional level and shall include key success criteria. The ENTSO for Electricity shall consult the Commission and may seek advice from ACER, ENISA and the Joint Research Centre on the organisation and execution of the regional and cross regional cybersecurity exercises.

Article 45

Outcome of cybersecurity exercises at entity, Member State, regional or cross regional levels

1. Upon request from a critical-impact entity, critical service providers shall participate in the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1) when they provide services for the critical-impact entity in the area corresponding with the scope of the relevant cybersecurity exercise.

2. The organisers of the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1), with the advice of ENISA if requested by them and pursuant to Article 7(5) of Regulation (EU) 2019/881, shall analyse and finalise the relevant cybersecurity exercise through a report summarising the lessons, addressed to all participants. The report shall include:

   (a) the exercise scenarios, meeting reports, main positions, successes and lessons learnt at any level of the electricity value chain;

   (b) whether the key success criteria were met;

   (c) a list of recommendations for entities participating in the relevant cybersecurity exercise to correct, adapt or change cybersecurity crisis processes, procedures, associated governance models and any existing contractual engagements with critical service providers.

3. If requested by the CSIRTs network or the NIS Cooperation Group or the EU CyCLONe, the organisers of the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1) shall share the outcome of the relevant cybersecurity exercise. The organisers shall share with each entity participating in the exercises the information referred to in paragraph 2, points (a) and (b) of this Article. The organisers shall share the list of recommendations referred to in that paragraph, point (c) exclusively with the entities addressed in the recommendations.

4. The organisers of the cybersecurity exercises referred to in Article 43(1) and (2) and in Article 44(1) shall follow up regularly with the entities participating in the exercises on the implementation of the recommendations pursuant to paragraph 2, point (c) of this Article.

CHAPTER VII

PROTECTION OF INFORMATION

Article 46

Principles for the protection of exchanged information

1. The entities listed in Article 2(1) shall ensure that information provided, received, exchanged or transmitted under this Regulation is accessible only on a need-to-know basis and in accordance with relevant Union and national rules on security of information.
2. The entities listed in Article 2(1) shall ensure that information provided, received, exchanged or transmitted under this Regulation is handled and tracked during the entire life-cycle of that information and that it may be released at the end of its life-cycle only after being anonymised.
3. The entities listed in Article 2(1) shall ensure that all necessary protection measures of organisational and technical nature are in place to safeguard and protect the confidentiality, integrity, availability and non-repudiation of information provided, received, exchanged or transmitted under this Regulation, independently from the means used. The protection measures shall:
   (a) be proportionate;
   (b) take into consideration cybersecurity risks related to known past and emerging threats to which such information may be subject in the context of this Regulation;
   (c) to the extent possible, be based on national, European or international standards and best practices;
   (d) be documented.
4. The entities listed in Article 2(1) shall ensure that any individual who is granted access to information provided, received, exchanged or transmitted under this Regulation is briefed on the security rules applicable at entity level and on the measures and procedures relevant to the protection of information. Those entities shall ensure that the concerned individual acknowledges the responsibility to protect the information as instructed during the briefing.
5. The entities listed in Article 2(1) shall ensure that access to information provided, received, exchanged or transmitted under this Regulation is limited to individuals:
   (a) who are authorised to access that information based on their functions and limited to the execution of the tasks assigned;
   (b) for whom the entity was able to assess ethical and integrity principles, as well as for whom there is no evidence of negative outcome from a background verification check to evaluate reliability of the individual in accordance with

the best practices and standard security requirements of the entity, and, where necessary, with the national laws and regulations.

6. The entities listed in Article 2(1) shall have the written agreement of the natural or legal person that originally created or provided the information, prior to providing that information to a third party that falls outside the scope of this Regulation.

7. An entity listed in Article 2(1) may consider that this information shall be shared without complying with paragraphs 1 and 4 of this Article in order to prevent a simultaneous electricity crisis with a cybersecurity root cause or any cross-border crisis within the Union in another sector. In that case, it shall:

   (a) consult and be authorised by the competent authority to share such information;

   (b) anonymise such information without losing the elements necessary to inform the public of an imminent and serious risk to cross-border electricity flows and the possible mitigation measures;

   (c) safeguard the identity of the originator and of the entities that have been processing such information under this Regulation.

8. By derogation from paragraph 6 of this Article, the competent authorities may provide information provided, received, exchanged or transmitted under this Regulation to a third party not listed in Article 2(1) without a written prior consent of the originator of the information but informing the latter at the earliest time possible. Before disclosing any information provided, received, exchanged or transmitted under this Regulation to a third party not listed in Article 2(1), the concerned competent authority shall reasonably ensure that the concerned third party is aware of the security rules in force and shall receive reasonable assurance that the concerned third party can protect the received information in compliance with paragraphs 1 to 5 of this Article. The competent authority shall anonymise such information without losing the elements necessary to inform the public of an imminent and serious risk to cross-border electricity flows and possible mitigations measures and safeguard the identity of the originator of the information. In this case, the third party not listed in Article 2(1) shall protect the received information in accordance with provisions already in force at entity level, or where this is not possible, with the provisions and instructions provided by the relevant competent authority.

9. This Article does not apply to entities not listed in Article 2(1) that are provided with information pursuant to paragraph 6 of this Article. In this case paragraph 7 of this Article shall be applied, or the competent authority may provide that entity with written provisions to apply in cases where information is received pursuant to this Regulation.

Article 47

Confidentiality of information

1. Any information provided, received, exchanged or transmitted pursuant to this Regulation shall be subject to the conditions of professional secrecy laid down in paragraphs 2 to 5 of this Article of this Regulation and requirements as laid down in Article 65 of Regulation (EU) 2019/943. Any information provided, received,

exchanged or transmitted among entities listed in Article 2 of this Regulation, for the purposes of implementing this Regulation, shall be protected, considering the confidentiality level of the information applied by the originator.

2. The obligation of professional secrecy shall apply to the entities listed in Article 2.

3. The CS-NCAs, the NRAs, the RP-NCAs and the CSIRTs shall exchange all necessary information to carry out their tasks.

4. Any information received, exchanged or transmitted among entities listed in Article 2(1), for the purposes of implementing Article 23, shall be anonymised and aggregated.

5. Information received by any entity or authority subject to this Regulation in the course of their duties may not be disclosed to any other entity or authority, without prejudice to cases covered by national law, other provisions of this Regulation or other relevant Union legislation.

6. Without prejudice to 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.

7. ACER, after consulting ENISA, all competent authorities, ENTSO for Electricity and the EU-DSO Entity, shall by [*OP: please insert the date = 12 months after the entry into force of this Regulation*] issue guidelines addressing mechanisms for all entities listed in Article 2(1) to exchange information, and in particular envisaged communication flows, and methods to anonymise and to aggregate information for the purpose of implementation of this Article.

8. Information that is confidential pursuant to Union and national rules shall be exchanged with the Commission and other relevant authorities only where that exchange is necessary for the application of this Regulation. The information exchanged shall be limited to that which is necessary and proportionate to the purpose of that exchange. The exchange of information shall preserve the confidentiality of that information and protect the security and commercial interests of critical-impact or high-impact entities.

CHAPTER VIII

FINAL PROVISIONS

Article 48

Temporary provisions

1. Until the approval of the terms and conditions or methodologies referred to in Article 6(2) or plans referred to in Article 6(3), the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop non-binding guidance on the following issues:

   (a) a provisional electricity cybersecurity impact index (‘ECII’) pursuant to paragraph 2 of this Article;

   (b) a provisional list of Union-wide high-impact and critical-impact processes pursuant to paragraph 4 of this Article; and

(c) a provisional list of European and international standards and controls required by national legislation with relevance for cybersecurity aspects of cross-border electricity flows pursuant to paragraph 6 of this Article.

2. By [*OP: please insert the date = four months after the entry into force of this Regulation*], the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop a recommendation for a provisional ECII. The ENTSO for Electricity, in cooperation with the EU DSO entity, shall notify the recommended provisional ECII to the competent authorities.

3. Four months of receipt of the recommended provisional ECII, or the latest by [*OP: please insert the date = eight months after entry into force*], the competent authorities shall identify candidates for high-impact and critical-impact entities in their Member State based on the recommended ECII and shall develop a provisional list of high-impact and critical-impact entities. The high-impact and critical-impact entities identified in the provisional list may voluntarily fulfil their obligations as laid down in this Regulation based on a precautionary principle. By [*OP: please insert the date = nine months after the entry into force of this Regulation*], the competent authorities shall notify the entities identified in the provisional list that they have been identified as a high-impact or critical-impact entity.

4. By [*OP: please insert the date = six months after entry into force of this Regulation*], the ENTSO for Electricity, in cooperation with the EU DSO entity, shall develop a provisional list of Union-wide high-impact and critical-impact processes. The entities notified pursuant to paragraph (3) that voluntarily decide to fulfil their obligations as laid down in this Regulation based on a precautionary principle shall use the provisional list of high-impact and critical-impact processes to determine the provisional high-impact and critical-impact perimeters and to determine which assets are to be included in the first cybersecurity risk assessment at entity level.

5. By [*OP: please insert the date = three months after entry into force*], each competent authority according to Article 4 (1) shall provide a list of its national legislation with relevance for cybersecurity aspects of cross-border electricity flows to the ENTSO for Electricity and the EU DSO entity.

6. By [*OP: please insert the date = 12 months after entry into force of this Regulation*], the ENTSO for Electricity, in cooperation with the EU DSO entity, shall prepare a provisional list of European and international standards and controls required by national legislation with relevance for cybersecurity aspects of cross-border electricity flows, taking into account the information provided by the competent authorities.

7. The provisional 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.

8. The ENTSO for Electricity and the EU DSO entity shall take into account the views provided by ENISA and ACER when finalising the provisional list of standards. The ENTSO for Electricity and the EU DSO entity shall publish the transitional list of European and international standards and controls on their websites.

9. The ENTSO for Electricity and the EU DSO entity shall consult ENISA and ACER on the proposals for non-binding guidance developed pursuant to paragraph 1.

10. Until the minimum and advanced cybersecurity controls are developed pursuant to Article 29 and adopted pursuant to Article 8, all entities listed in Article 2(1) shall strive to progressively apply the non-binding guidance developed pursuant to paragraph 1.

Article 49

Entry into force

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

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

Done at Brussels, 11.3.2024

For the Commission
The President
Ursula VON DER LEYEN