Energy Community

PROCEDURAL ACT OF THE MINISTERIAL COUNCIL OF THE ENERGY COMMUNITY

2018/2/MC-EnC: on the Establishment of an Energy Community Coordination Group for Cyber-Security and Critical Infrastructure

The Ministerial Council of the Energy Community,

Having regard to the Treaty Establishing the Energy Community, and in particular Articles 86 and 87 thereof,

Having regard to Articles 2 and 3 of the Treaty Establishing the Energy Community calling for the enhancement of the security of supply of the single regulatory space in the Energy Community, and access for all Contracting Parties to a stable and continuous energy supply that is essential for economic development and social stability;

Whereas due to the proliferation of information and communication technologies in the energy sector, cyber-security matters have become an intrinsic part of a number of existing Energy Community acquis, that deal with the security of supply or safe operation of energy systems,

Whereas the stabilization and association agreements of the European Union and its Member States with Albania, Bosnia and Herzegovina, former Yugoslav Republic of Macedonia, Kosovo*[1], Montenegro, and association agreements with Georgia, Moldova and Ukraine require these Contracting Parties adopt a series of European Union legislation on cybersecurity matters and protection of critical infrastructure, including in the energy sectors,

Whereas there are certain critical infrastructures in the Energy Community, the disruption or destruction of which would have significant cross-border impacts or cross-sectoral effects resulting from interdependencies between interconnected infrastructures and systems, which require the setting-up of a coordination mechanism at Energy Community level,

Whereas timely and effective response to incidents relies on the existence of previously established and, to the extent possible, well-rehearsed cooperation procedures and mechanisms having clearly defined the roles and responsibilities of the key actors at national and Energy Community level,

Whereas an effective organizational framework for a high level of security of information systems and critical infrastructures requires taking an all-hazard approach where man-made, technological threats and natural disasters need all to be taken into account in the protection process,

Whereas a Community approach will encourage private sector involvement in overseeing and managing risks, business continuity planning and post-disaster recovery,

Whereas existing sectoral measures at national level require coordinated regional action through Community mechanisms, with a view to enhancing effectiveness, avoid duplication of, or contradiction between, different acts or measures,

[1] This designation is without prejudice to positions on status, and is in line with UNSCR 1244 and the ICJ Opinion on the Kosovo.

Whereas cyber-security calls for a group of experts to advise the Energy Community, the national institutions as well as to coordinate incident and crisis management measures,

Whereas such a group should be composed of all relevant stakeholders and should cover electricity, gas and oil sectors, encompassing generation, distribution, transmission and supply,

Upon proposal of the Secretariat,

HAS ADOPTED THIS PROCEDURAL ACT:

Article 1

1. To promote a high level of security of network and information systems and of critical infrastructures within the Energy Community, a coordination group for cyber-security and critical infrastructure ("CyberCG") is hereby established.

2. Each Party shall designate and notify to the Energy Community Secretariat one or more national competent authorities as well as a single point of contact for the security of network and information systems and of critical infrastructures ('competent authority' and 'single point of contact'), covering at least the sectors referred to in referred to in point 2. e) of the Annex.

3. Each Party shall designate and notify to the Energy Community Secretariat one or more national computer security incident response teams ('CSIRTs').

4. The CyberCG shall

(a) perform its tasks as described in the Annex to the present Procedural Act;
(b) liaise with a network of CSIRTs as described in the Annex to the present Procedural Act;
(c) liaise with security liaison officer for each critical infrastructure in Contracting Parties.

5. The activities of the CyberCG shall be governed by Terms of Reference stipulated in the Annex to this Procedural Act.

6. This article is without prejudice to the actions taken by the Parties to safeguard their essential State functions, in particular to safeguard national security, including actions protecting information the disclosure of which Parties consider contrary to the essential interests of their security, and to maintain law and order, in particular to allow for the investigation, detection and prosecution of criminal offences.

Article 2

This Procedural Act shall enter into force on the day of its adoption and is addressed to the Parties to the Energy Community.

Done in Skopje, on 29 November 2018

For the Ministerial Council

.....

Presidency

ANNEX: Terms of Reference of the Energy Community cyber-security and critical infrastructure cooperation group (CyberCG)

This document describes the organizational structure, activities and the responsibilities of all parties concerned within the coordination group for cyber-security and critical infrastructure ("CyberCG").

1. General

The CyberCG aims to support and facilitate strategic cooperation and the exchange of information within the Energy Community and to develop trust and confidence, and with a view to achieving a high common level of security of network and information systems and of critical infrastructures in the Energy Community.

2. Definition of Terms

For the purposes of the present Annex, the following definitions apply:

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

b) 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;

c) 'national strategy on the security of network and information systems' means a framework providing strategic objectives and priorities on the security of network and information systems at national level in accordance with requirements of Article 7 of Directive 2016/1148/EU;

d) 'operator of essential services' means a public or private entity which provides an energy service that (i) is essential for the maintenance of critical societal and/or economic activities, (ii) the provision of that service depends on network and information systems, (iii) and an incident would have significant disruptive effects on the provision of that service, in accordance with the criteria laid down in Article 5(2) of Directive 2016/1148/EU;

e) 'energy services' comprise (i) electricity generation, supply, market operation, distribution, transmission, and storage, (ii) natural gas production, supply, market operation, transmission, distribution, storage and LNG, (iii) oil production, refining and treatment facilities, market operation, storage and transmission, (iv) monitoring and control of pollution and emissions from energy combustion and (v) digital services and electronic communication services, in case and to the extent that the latter provide services to operators of essential services of the energy sectors, and/or that provide services that are essential to the functioning of the energy sector";

f) 'critical infrastructure' means an asset, system or network or part thereof within the energy sector or interdependent with the energy services referred to in point e), located in Contracting Parties

which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, the disruption or destruction of which would have a significant impact in a Contracting Party as a result of the failure to maintain those functions;

g) 'Energy Community critical infrastructure' means critical infrastructure located in Contracting Parties the disruption or destruction of which would have a significant impact on at least two Contracting Parties and/or Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure;

h) 'owners/operators of critical infrastructures' means those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as a critical infrastructure in the relevant Contracting Parties. For the avoidance of doubt, the definition of an operator of critical infrastructure encompasses and is broader than that of an operator of essential services, as it covers also critical infrastructures that do not depend on information network and systems;

i) 'incident' means any event having an actual adverse effect on the security of network and information systems within the meaning of Directive 2016/1148/EU or any event causing a disruption or destruction of critical infrastructure installations within the meaning of Directive 2008/114/EC;

j) 'incident handling' means all procedures supporting the detection, analysis and containment of an incident and the response thereto, as provided under Directive 2016/1148/EU and related implementing acts;

k) 'risk' means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems, as provided under Directive 2016/1148/EU and related implementing acts, or having the potential of causing a disruption or destruction of critical infrastructure installations as provided under Directive 2008/114/EC, including cyber-attacks, natural disasters, terrorist attacks or any other sources of attack.

l) 'risk analysis' means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure or network and information systems,;

m) 'protection' means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralize a threat, risk or vulnerability;

n) 'standard' means a standard within the meaning of point (1) of Article 2 of Regulation No 1025/2012/EU;

o) 'specification' means a technical specification within the meaning of point (4) of Article 2 of Regulation No 1025/2012/EU.

3. Composition

3.1. The CyberCG consists of representatives of the Parties (competent authorities and single point of contacts), the CSIRTs network, security liaison officers, the Secretariat, the European Commission, and the European Union Agency for Network and Information Security ("ENISA").
3.2. Representatives of Observer and Participant countries may participate in the CyberCG.
3.3. Where appropriate, the CyberCG may invite representatives of the relevant stakeholders to participate in its work.

3.4. The Secretariat shall provide assistance and logistical support to the CyberCG.

4. Single points of contact

4.1. The single points of contact exercises a liaison function to ensure cross-border cooperation of Parties' authorities and with the relevant authorities in other Parties, with the CyberCG and the CSIRTs network. Tasks of the single point of contact may be assigned to the competent authority.

4.2. Single points of contact notify and report to the CyberCG, the CSIRTs network and the Secretariat, by 15 January 2019, and every year thereafter, on provisions of national law and measures in the fields covered by point 2. e) of this Annex, including but not limited to:

a) adoption of a national strategy on the security of network and information systems covering at least the sectors point 2. e) of this Annex, in compliance with requirements set forth in Article 7 of Directive 2016/1148/EU, and adoption of security strategies or equivalent instruments on the protection of critical infrastructures from other risks, not covered by national strategy on the security of network and information systems, in compliance with requirements laid down in Directive 2008/114/EC;

b) on the identification of operators of essential services for sectors and services referred to in point 2.e) of this Annex, in compliance with requirements of Articles 5 and 6 of Directive 2016/1148/EU; on security and incident notification requirements that those operators of essential services shall implement, in compliance with requirements laid down in Article 14 of Directive 2016/1148/EU; as well as on enforcement powers and means given to competent authorities in this respect, in compliance with requirements laid down in Article 15 of Directive 2016/1148/EU;

c) on security requirements and incident notification obligations that entities operating organized energy trading and balancing services' platforms as referred to in point 2. e) of this Annex implement, in compliance with requirements laid down in Directive 2016/1148/EU; or in compliance with security requirements equivalent to those laid down in Directive 2014/65/EU on markets in financial instruments, supplemented by any implementing acts, or equivalent to those laid down in Regulation 600/2014/EU, as supplemented by any implementing acts, as well as national provisions on enforcement powers and means given to competent authorities in this respect;

d) on security requirements and incident notification obligations that digital service providers referred to in point 2. e) of this Annex implement, in compliance with requirements laid down in Article 16 of Directive 2016/1148/EU; as well as national provisions on enforcement powers and means given to competent authorities in this respect, in compliance with requirements laid down in Article 17 of Directive 2016/1148/EU;

e) on security requirements and incident notification obligations that electronic communications operators referred to in point 2. e) of this Annex implement, in compliance with requirements laid down in Articles 13a and 13b of Directive 2002/21/EC,; as well as national provisions on enforcement powers and means given to competent authorities in this respect, in compliance with requirements laid down in Articles 13a and 13b of Directive 2002/21/EC;

f) on the identification of critical infrastructures located on the territory of the concerned Contracting Party, on security measures and operational plans that are implemented to ensure a level of security and protection of critical infrastructures for sectors and services referred to in point 2. e) of this Annex, in compliance with requirements equivalent to those laid down in Article 5 and Annex II of

Directive 2008/114/EC, for risks and incidents that are not covered by the above-mentioned from b) to e), as well as on enforcement powers and means given to competent authorities in this respect.

5. Tasks

5.1. The CyberCG covers the following tasks:

a) providing strategic guidance for the activities of the CSIRTs established and the CSIRTs network;

b) exchanging best practice on the exchange of information related to incident notification within the meaning of or equivalent to provisions in Article 14(3) and (5) and Article 16(3) and (6) of Directive 2016/1148 EU, and/or to the identification of critical infrastructures in the Contracting Parties for at least the sectors referred to in point 2. e) of this Annex;

c) exchanging best practice between Parties and other stakeholders involved;

d) assisting Contracting Parties in building capacity to ensure the security of network and information systems, and in securing critical infrastructures;

e) discussing capabilities and preparedness of the Contracting Parties, and evaluating national strategies on the security of network and information systems and the effectiveness of CSIRTs, and of critical infrastructures protection and identifying best practice;

f) exchanging information and best practice on awareness-raising and training;

g) exchanging information and best practice on research and development relating to the security of network and information systems and to the protection of critical infrastructures;

h) where relevant, exchanging experiences on matters concerning the security of network and information systems and of critical infrastructures, with relevant Energy Community institutions, in particular the Secretariat and the Energy Community Security of Supply Coordination Group;

i) discussing the standards and specifications with relevant stakeholders and with relevant organizations where appropriate;

j) collecting best practice information on risks and incidents;

k) examining, on an annual basis, the reports submitted;

l) discussing the work undertaken with regard to exercises relating to the security of network and information systems and of critical infrastructures, education programmes and training;

m) exchanging best practice with regard to the identification of operators of essential services by the Contracting Parties, identification of critical infrastructures, including in relation to cross-border dependencies, and cross-sectoral dependencies regarding risks and incidents, where appropriate with the assistance of the Energy Community Security of Supply Coordination Group, building on the best practice of ENISA;

n) engaging in discussions with the Contracting Party, or Contracting Parties and Member States on whose territory a potential critical infrastructure is located, and with the other Contracting Parties and Member States which may be significantly affected by the potential critical infrastructure, providing guidance for the identification of critical infrastructures or of operator of essential service and where

necessary facilitating agreements between the concerned Contracting Parties and Member States on common security and protection measures;

o) discussing modalities for reporting notifications of incidents;

p) developing common methodological guidelines for carrying out risk analyses in respect of Energy Community critical infrastructures. The CyberCG shall support, through the relevant Contracting Party's competent authority/single point of contact, the owners/operators of critical infrastructures by providing access to available best practices and methodologies as well as support training and the exchange of information on new technical developments related to critical infrastructure protection;

q) promoting convergent implementation of security requirements of network and information systems and of critical infrastructures, without imposing or discriminating in favour of the use of a particular type of technology,

r) encouraging the use of European or internationally accepted standards and specifications relevant to the security of network and information systems.

5.2. The CyberCG shall carry out its tasks on the basis of biennial work programmes. The work programme shall outline actions to be undertaken to implement the CyberCG's objectives and tasks.

5.3. The CyberCG shall take part in the meetings and activities of the SoS CG, where appropriate.

5.4. The CyberCG shall prepare a report assessing the experience gained with the strategic cooperation by October 2019, and every year thereafter, and submit it to the Secretariat, so that the latter uses it for the preparation of its implementation report for the Ministerial Council.

6. Chairs

The Cyber-CG shall nominate and appoint a Chairperson and two Vice Chairpersons for a period of two years.

7. Meetings of the Cyber-CG

7.1. The Cyber-CG will meet when considered necessary upon a motion of the Chairperson, the Chairperson of Energy Community Security of Supply Coordination Group, the Secretariat, or ENISA. The Cyber-CG will normally meet twice a year.

7.2. A draft agenda will be distributed at least two weeks before each meeting. Draft conclusions will be distributed within two weeks after the meeting for approval by the members.

7.3. The Secretariat will prepare and organize workshops, when considered useful, following the conclusions of the Cyber-CG.

8. Computer security incident response teams (CSIRTs)

8.1. CSIRTs designated by Contracting Parties covering at least the sectors referred to in in point 2. e) of this Annex, responsible for risk and incident handling in accordance with a well-defined process. CSIRTs could also be established within the competent authority.

8.2. CSIRTs should have access to an appropriate, secure, and resilient communication and information infrastructure at national level in accordance with requirements of Directive 2016/1148.

8.3. Contracting Parties shall inform the Secretariat and the CyberCG about the remit, as well as the main elements of the incident-handling process, of their CSIRTs.

8.4. Contracting Parties may request the assistance of the CyberCG in developing national CSIRTs.

9. CSIRTs Network

9.1. In order to promote swift and effective operational cooperation in cases of risks or incidents to information and communications networks and systems, a network of the national CSIRTs is established.

9.2. The CSIRTs Network shall be composed of representatives of the Contracting Parties CSIRTs. The Secretariat shall participate in the CSIRTs network.

9.3. The CSIRTs network shall have the following tasks:

a) exchanging information on CSIRTs' services, operations and cooperation capabilities;

b) at the request of a representative of a CSIRT from a Contracting Party potentially affected by an incident, exchanging and discussing non-commercially sensitive information related to that incident and associated risks; however, any Contracting Party's CSIRT may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident;

c) exchanging and making available on a voluntary basis non-confidential information concerning individual incidents;

d) at the request of a representative of a Contracting Party's CSIRT, discussing and, where possible, identifying a coordinated response to an incident that has been identified within the jurisdiction of that same Contracting Party;

e) providing Contracting Parties with support in addressing cross-border incidents on the basis of mutual assistance, including under Chapter IV, Title IV of the Energy Community Treaty

f) discussing, exploring and identifying further forms of operational cooperation, including in relation to: (i) categories of risks and incidents; (ii) early warnings; (iii) mutual assistance; (iv) principles and modalities for coordination, when Contracting Parties respond to cross-border risks and incidents;

g) informing the CyberCG of its activities and of the further forms of operational cooperation discussed pursuant to point (f), and requesting guidance in that regard;

h) discussing lessons learnt from exercises relating to the security of network and information systems, including from experience shared by ENISA;

i) at the request of an individual CSIRT, discussing the capabilities and preparedness of that CSIRT;

j) issuing guidelines in order to facilitate the convergence of operational practices and operational cooperation;

k) developing a blueprint for cooperation at Energy Community level in case of incidents or crisis affecting one or more Contracting Parties to such an extent that an intervention at Energy Community level is required.

9.4. The CSIRTs network produces an annual report assessing the experience gained with the operational cooperation, including conclusions and recommendations. That report shall be submitted to the CyberCG.

9.5. The CyberCG and the Secretariat shall actively support the cooperation among the CSIRTs. The CSIRTs shall build on best practice of ENISA in performing its tasks and duties, and where appropriate and possible may seek assistance from ENISA.

10. Closed-CSIRT network

10.1. Within the CSIRT network, a closed-CSIRT network is established to treat such a threat and risk landscape and incidents that are considered as classified information by the Contracting Parties concerned. The closed-CSIRT network is composed of a representative from each Contracting Party which shall have an appropriate level of security vetting and clearance equivalent to that of handling classified information at European Union level.

10.2. The closed-CSIRT network shall make use of specific certified communication means that provide a secure way to communicate the classified information. The same applies to non-written information exchanged during meetings of the closed-CSIRT network.

11. Security liaison officer for critical infrastructures

11.1. Contracting Parties should designate one security liaison officer for security issues for each critical infrastructure. The security liaison officer functions as the point of contact between the owner/operator of the Energy Community critical infrastructure, the relevant Contracting Party's competent authority/single point of contact and the Cyber-CG.

11.2. Contracting Parties shall inform the Energy Community Secretariat and the Cooperation Group about the remit, as well as the main elements of the incident- handling process, of their security liaison officers.

12. Competent authorities, single point of contacts, CSIRTs and security liaison officers

12.1. Competent authorities, single points of contact, CSIRTs and security liaison officers should have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them.

12.2. Competent authorities, single points of contact, CSIRTs and security liaison officers, whenever appropriate and in accordance with national law, consult and cooperate with the relevant national law enforcement authorities and national data protection authorities.

13. Cooperation with ENISA (European Union Agency for Network and Information Security)

By 1 July 2019, the CyberCG shall explore possibilities and options for Contracting Parties and the Secretariat to engage as observer with ENISA on issues related to cybersecurity in Network Energy, and participate in the international activities organized by ENISA.