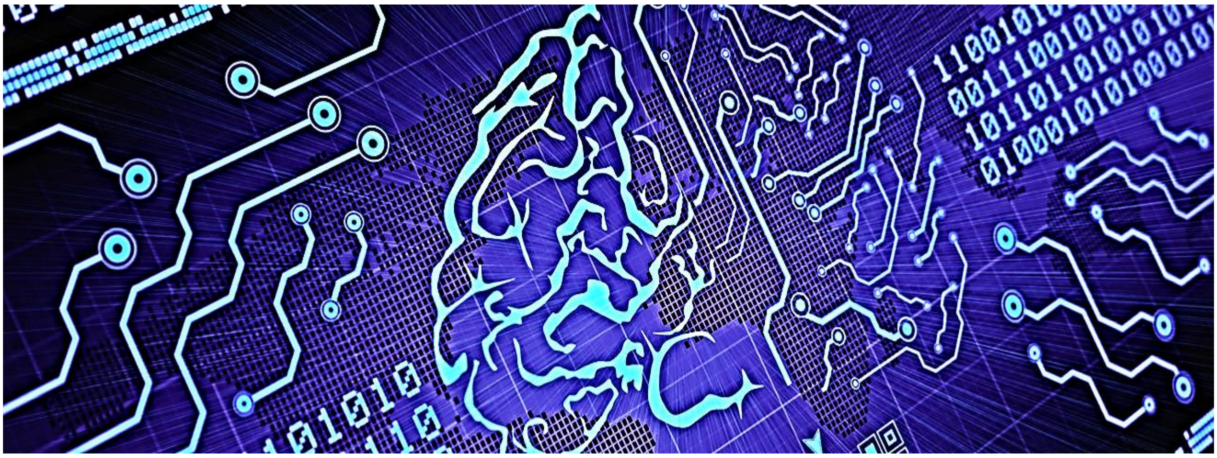
Energy Community

Draft 02v1 – 20 November 2019

ENERGY COMMUNITY COORDINATION GROUP on CYBERSECURITY and CRITICAL INFRASTRUCTURES

WORK PROGRAMME 2020 – 2021



Vienna, December 2019

This **Work Programme** is developed pursuant to Point 5.2 of the “Terms of Reference of the Energy Community Cybersecurity and Critical Infrastructures Cooperation Group” (CyberCG ToR) adopted by the Energy Community Ministerial Council in November 2018 as Annex of the Procedural Act on the Establishment of the CyberCG, and Item 1 of the Conclusions from the first CyberCG Meeting of 11 April 2019. It consists of a general part on the common terms and conditions of the CyberCG operation, and a set of **Work Plans** (annex) referring to the tasks and activities addressing specific targets and working groups / categories of stakeholders.

The proposed schedule of the Work Plan and the corresponding events (meetings, conferences, training sessions, panels, etc.) as well as the indicated technical assistance are tentative only and may be modified at any time according to the interest of the CyberCG parties, co-organization of events, and possible EnC Secretariat’s budgetary or other constraints.

Contents

INTRODUCTION 4
ORGANIZATION 4
TASKS 8
PLANNING and REPORTING 8
ANNEX 1 9
WORK PLAN 2020 - 2021 9
ANNEX 2 14
Working Group on Energy Community Critical Infrastructures WORK PLAN 2020 - 2021 14
COMPOSITION 14
DESCRIPTION 14
SCOPE OF ACTIVITY 16
TASK 1 – Identification and designation of critical energy infrastructures 16
TASK 2 – Operator Security Plans (OSP) 18
ANNEX 3 22
Working Group on Cybersecurity Governance WORK PLAN 2020 - 2021 22
COMPOSITION 22
DESCRIPTION 22
SCOPE OF ACTIVITY 24
TASK 3 – EU acquis on cybersecurity for adoption in the Energy Community 24
TASK 4 – Energy Cybersecurity Strategies in the Energy Community 27
TASK 5 – Regulatory treatment of Cybersecurity in energy 29
TASK 6 – Technical standards for cybersecurity in energy 32
ANNEX 4 35
Energy Community Cybersecurity Networks WORK PLAN 2020 - 2021 35
COMPOSITION 36
DESCRIPTION 36
SCOPE OF ACTIVITY 38
TASK 7 –Energy Community CSIRT Network 38
TASK 8 – Energy Community Energy ISAC 44

INTRODUCTION

The Procedural Act 2018/PA/2 /MC-EnC[1] adopted by the Energy Community Ministerial Council on 29 November 2018 established the Coordination Group for Cybersecurity and Critical Infrastructures (CyberCG), and addressed the Parties[2] of the Energy Community for their participation. The Procedural Act defines the organizational structure of CyberCG, its tasks, activities and responsibilities of the Parties, and provides the legal background for this Work Programme.

CyberCG is established to promote a high level of security of network and information systems and of critical energy infrastructures within the Energy Community, aiming to support and facilitate strategic cooperation and the exchange of information and develop trust and confidence. It provides an environment for open discussion between the interested parties (government, NRA, operators, service providers and security teams) on shared concerns or questions of common interest.

CyberCG respects the national rules for protection of confidential information, and relies on mutual responsibility and measure of discretion for all representatives required to enable effective cooperation and shared results.

The activities of CyberCG are without prejudice to the actions taken by the Parties to safeguard their essential State functions and interests, in particular to safeguard national security, including actions protecting information the disclosure of which Parties consider contrary to the essential interests of their security.

ORGANIZATION

The CyberCG consists of representatives of the Parties, designated by the Parties and notified to the Energy Community Secretariat, including:

1) representatives of competent authorities – relevant ministries and national regulatory authorities;
2) single points of contact for the security[3] of network and information systems substantial for the operation of critical infrastructures[4] and/or provision of essential services[5] at least in the energy sectors defined herewith, and
3) one or more national computer security incident[6] response teams (CSIRT-s) with responsibility in energy

The energy sectors[7] relevant for critical infrastructures and essential services include:

- electricity generation, transmission, distribution, storage, supply, market operation;
- natural gas production, transmission, distribution, storage, LNG, supply, market operation;
- oil production, refining / treatment, transmission, storage, market operation;

[1] https://www.energy-community.org/dam/jcr:a9163c92-fb05-40c3-a74c-acca91fe94c1/PA_02_2018_MC-EnC_CSCG_112018.pdf

[2] - as identified in the Energy Community Treaty Preamble (http://ec.europa.eu/world/agreements/downloadFile.do?fullText=yes&treatyTransId=4181)

[3] - as defined in Point 2(a), (b) of the CyberCG Terms of Reference

[4] - as defined in Point 2(f), (g), (h) of the CyberCG Terms of Reference

[5] - as defined in Point 2(d) of the CyberCG Terms of Reference

[6] - as defined in Point 2(i), (j) of the CyberCG Terms of Reference

[7] - as identified in Point 2(e) of the CyberCG Terms of Reference

- monitoring / control of pollution and emissions from combustion;
- digital / electronic communication services provided to operators of essential energy services / critical infrastructures, or otherwise estimated as essential for functioning of the energy sector

The representatives from each of these sectors participate in the plenary meetings, public events and in the sectoral activities and events according to their professional preferences.

CyberCG also includes the Energy Community Secretariat, the European Commission, and the European Union Agency for Network and Information Security (ENISA). Representatives of Observer and Participant countries may also participate. Upon invitation from CyberCG, the Secretariat, the European Commission, or ENISA representatives of other relevant stakeholders may participate in its work.

The CyberCG operates in the following formats:

- plenary meetings
- working groups
- capacity building format
- direct communication domain
- public communication domain

The **Plenary meetings** take place twice a year, following Items 7(1), (2) of the ToR. They address the overall Group structure (focal points, liaison officers, official representatives of stakeholders and CSIRTs), on general topics of CyberCG operation and organization.

Ordinary meetings include updates on cybersecurity developments on national, regional and EU level. They enable discussion and adoption of measures, policies and specific deliverables of the Working Groups (reports, rules, recommendations, policy papers), as well as adoption of decisions on its structure, work plans, schedules, policies, programmes and other acts, and consultation on topics of general interest for cybersecurity in the Energy Community.

Extraordinary meetings have special agenda addressing the reasons for calling the meeting, and includes discussion and decisions on the activities or mechanisms for overcoming the culprits.

The Plenary meetings are chaired by an appointed chairperson. Following Item 6 of the ToR, a Chairperson and two Vice Chairpersons of the CyberCG are appointed for a period of two years. Assisted by the Secretariat, they chair and co-chair the plenary meetings, and endeavour to ensure full representation and participation by all Parties and efficient operation of the Coordination Group in all activities.

The Secretariat provides technical support and guidance in organization of the activities of the Group, set-up of the events and cooperation with third parties. The secretariat develops the draft acts (agendas, decisions, conclusions, plans, reports and other working papers), and publishes the adopted acts. The Secretariat also provides legal assistance on cybersecurity in energy on national level for the Energy Community Contracting Parties – assessment of laws, policies and other acts of governance, and develops draft proposals for the deliverables (relevant documents and papers developed by the Coordination Group.

Working Groups (WG) are the main format of cooperation between the CyberCG Parties in completion of the CyberCG tasks. CyberCG brings a Decision on the establishment of a WG upon a proposal from the Chairperson or the Secretariat. The WG participants consist of representatives of the Parties coming from the sectors relevant for accomplishment of the tasks, the Secretariat, relevant EU institutions and experts. Additional representatives from specific stakeholders may be included in the WG if required.

The Working Group may apply an instrument (statement) for protection of the confidential information in the course of its activities.

The format, structure, targets and activities (along with corresponding timeline) for each Working Group are defined in a biannual **Work Plan** considered as a part of this Work Program. WG activities are focused on achieving specific set of related targets, which may include a review or design of draft acts (studies, reports, guidelines, rules, recommendations, templates, regulatory or legislative acts, strategies, agreements, etc.). The WG reports to CyberCG on its progress, submits the reviews or own draft acts and other deliverables for further consideration and proposes decisions. The WG sets its own schedule for meetings and other milestones – within the scope of its Work Plan and the overall deadlines, and decides on the allocation of individual activities among the participants on voluntary basis.

The work of the WG is guided by a convenor selected and appointed by the CyberCG and supported by the Secretariat. The convenor decides on micromanagement of the WG activities, meetings and communication within the WG. The convenor is responsible for timely completion of the activities, tasks and specific deliverables, and reports to the CyberCG.

The Secretariat provides the Working Groups the necessary technical assistance and support required for effective performance – as defined by the Work Plan or decided by the CyberCG, and to the limit of its available resources. Upon decision of CyberCG, the Secretariat shall endeavour to facilitate engagement of external expert resources or outsourcing some activities.

In addition to WG performance, CyberCG performs a set of “horizontal” activities (applicable to all groups of stakeholders and cybersecurity topics), which cover at least the domains of capacity building and communication. CyberCG may decide to include other horizontal activities of similar nature.

The **capacity building** activities of the CyberCG are defined in a dedicated biannual Programme that is a part of this Work Program, and include workshops, seminars and conferences, panel meetings on specific topic, training events and exercises. The Programme provides a tentative schedule of the events updated at each CyberCG meeting, depending on available experts or the timing of related events.

These events are dedicated to representatives from specific sectors, and organized by the Secretariat. The Programme is developed and maintained by the Secretariat and adopted by the CyberCG. To the extent the Programme involves regulatory aspects and/or the need for knowledge building of regulators in the context of cybersecurity, the Program will be coordinated with the annual work programme of the Energy Community Regulatory Board (ECRB) and the Energy Community Regulatory School. In the implementation of the Plan the Secretariat takes stock of parallel events and activities organized by EC, ECRB, the Energy Community Regulatory School, ENISA, ENTSO-E, ENTSO-G, ACER, CEER, other cybersecurity authorities in the EU and abroad and academia, as well as the means of cooperation and available technical assistance provided by the donor community (the World Bank, USAID, etc.). The Secretariat reports to CyberCG on the completed events and achieved results.

Direct communication activities are complementary to the working groups and address relatively smaller communities of stakeholders focussed on specific common problems. They include CSIRT panel (network) and establishment of Information Sharing and Analysis Centres (ISACs) including representatives from different companies within the same or related sectors (electricity, gas, oil, environment, etc.). These permanent panels apply periodic dedicated meetings, education and training facilities and online platforms for exchange of information. Another form of direct cooperation are joint regional risk preparedness exercises following specific risk scenarios and including stakeholders and CSIRTs from several countries from the Energy Community and the EU.

The activities of the CSIRTs supported by the CyberCG are indicated in Items 8 and 9 of the ToR.

This form of cooperation is applied within closed communities exchanging confidential or sensitive information and sharing highly professional and sophisticated knowledge, in both cases applying restricted access for the broader community. The panels are established by the CyberCG and operate according to Work Plans adopted by the CyberCG as part of this Work Programme.

CyberCG establishes communication mechanisms with other Energy Community groups. Following Item 5.3 of the ToR, CyberCG cooperates primarily with the Security of Supply Coordination Group (SoS CG). In a similar manner, the Group communicates with the Energy Community Regulatory Board (ECRB) via the ECRB Section at the Secretariat, the ECRB President and ECRB Vice-Presidency as well as the chairpersons of the ECRB working groups and the Energy Community Distribution System Operators (ECDSO) Coordination Group, on the related subjects matter. The cooperation includes coordinated activities, events, joint meetings reviews, studies and conferences, as well as regular exchange of information (reports, decisions, plans, etc.). Specific modes of cooperation or events are proposed by the Secretariat.

The Secretariat facilitates this form of cooperation and supports the activities on establishment and operation of Energy Community ISACs, development of a CSIRT network in the Energy Community and operation of communication tools, at the same time taking stock of the available expertise and capacity building resources provided by the CSIRT community. The Secretariat facilitates the participation into relevant EU-established events including CSIRTs and ISACs communities. Further to that, the Secretariat facilitates organization of thematic conferences and training seminars for the professional cybersecurity community mainly through the available technical assistance.

The Secretariat endeavours to host closed communication platforms established for the purpose of the panels and other direct communication purposes to the level such services can be met by the available technology, and to support, coordinate and promote bilateral or regional projects for application of the required technologies.

The domain of **public communication** includes public reports on the CyberCG activities and milestones, dedicated reports and publicly available materials produced by the Working Groups and adopted by the WG, other reports, publications, PR events, cooperation with other expert groups and conferences targeting cybersecurity. A specific activity in the public domain includes open events / workshops aimed at raising the awareness on cybersecurity and promotion of the basic criteria for resilience and cyber protection. These activities are structured in annual Plans and Event Schedule adopted by the CyberCG.

The Secretariat coordinates the public communication activities of the CyberCG, prepares the draft Plans and Schedules, and provides technical assistance for the events and the online PR. The hosting and maintenance of the CyberCG web-domain is done by the Secretariat, on its webpage.

TASKS

The tasks and activities of the CyberCG are defined in Item 5 of the ToR. The activities for the period 2020 - 2021 are outlined in Annex 1, and defined in substantial detail in the complementary Work Plans provided in the annex.

CyberCG may adopt a decision to accomplish other tasks or perform other activities related to cybersecurity in the energy sector. They shall relate primarily to the EU legislation on cybersecurity and on critical infrastructures, and the acts and reports adopted by the European Commission, ACER, ECRB, ENISA, ENTSO-E, ENTSOG and other bodies and organizations implementing the cybersecurity policy in the EU. Tasks may also be defined through decisions and recommendations of the Energy Community Ministerial Council (EC-MC), Permanent High Level Group (PHLG), the Energy Community Regulatory Board (ECRB), or the Security of Supply Coordination Group (SoS CG).

Specific Tasks and activities of the **Working Groups** are defined in more detailed in the corresponding Work Plans provided as part of this Programme.

The domain with legal relevance for mandatory representation in the Working Groups covers the territories of Energy Community Contracting Parties and Observers, while the implementation and participation in the Working Groups also include the territories of the EU Member States in the geographic scope[8] of the Energy Community Treaty Title III.

PLANNING and REPORTING

Following Item 5.4 of the ToR the CyberCG shall adopt an Annual Report addressing its administrative status, the accomplished tasks and state of planned activities, progress made by the Parties in implementation of the legal framework and cybersecurity policies,

The convenors of the Working Groups, assisted by the Secretariat, prepare annual reports of their Working Groups by 31 October each year and submit them to CyberCG. These reports, together with information on the parallel activities within the Group, are embedded in the CyberCG Annual Report.

The Secretariat, assisted by the CyberCG Chairpersons, prepares a draft Annual Report and submits it to CyberCG for adoption by 15 November each year, and publishes the adopted Report.

Following Item 4.2 of the ToR the representatives of the Parties stakeholders / “single points of contact” provide reports to CyberCG, by 15 January each year, on the legal framework and measures on all the items stipulated therein including plans for activities in the course of the year.

Based on the findings in the Annual Report and received information pursuant Item 4.2 of the ToR the Secretariat, by 20 January each year, updates the Work Plans for the Working Groups and the overall CyberCG Work Programme for the current year and proposes the activities for the next calendar year, and submit them to the CyberCG for comments. The adopted Plans for the current and the next year are published by 31 January.

[8] *(Hellenic Republic, Hungary, Bulgaria, Croatia, Italy, Poland, Romania and Slovakia)*

ANNEX 1

WORK PLAN 2020 - 2021

ACTIVITIES

In the planning period 2020 – 2021, the CyberCG shall endeavour on accomplishment of the following activities and targets:

1) establishment and maintenance of its organizational structure, appointment of points of contact for the national authorities and/or liaison officers for critical infrastructures pursuant to Article 1 of the Procedural Act and Points 4 (1) and (2) of its Annex, adoption of reports and plans, decisions on activities, documents and events, networking and exchange of information on cybersecurity-related developments at national level, etc.;
2) the Tasks within the Working Group (WG) on Energy Community Critical Infrastructures identified in the Work Plan 2020 – 2021 for this WG (an annex to this WP);
3) the Tasks within the Working Group (WG) on Cybersecurity Governance identified in the Work Plan 2020 – 2021 for this WG (an annex to this WP);
4) the Tasks within the Energy Community SCIRT Network identified in the corresponding Work Plan 2020 – 2021 (an annex to this WP);
5) Education and Training Program - related to points 2), 3) and 4), and other related activities planned and conducted in cooperation with external sources of support

The activities under 5) include organization / hosting of conferences, workshops, training sessions and exercises, seminars, discussion panels, lectures and other forms of capacity building mechanisms of rising awareness in the domain of cybersecurity, under the common umbrella of the Cybersecurity Academy of the Energy Community. On behalf of the Energy Community, these activities are planned and implemented by both ECS and / or ECRB. The activities include the following three categories:

(i) workshops or training sessions scheduled and organized in the course of implementation of the activities under 2), 3) and 4) – both related to engaged technical assistance, stocktaking exercises or consultation / promotion of deliverables;

(ii) ad-hock education and training events organized by ECS, focused on specific questions in the domain of cybersecurity – following the interest of groups or stakeholders, or for raising awareness in the public domain;

(iii) training / education events and conferences co-organized with parties from the energy / cybersecurity domain, relevant EU institutions or partners from the donor community

RESSOURCES

The drafting activities for all initial drafts and their later versions for all acts identified as deliverables within the Work Plans for the Activities under 2), 3) and 4), along with the draft acts (Procedural Acts, Decisions) required for their adoption by the Energy Community Governance bodies shall be accomplished by the Secretariat.

The organization and hosting of all meetings related to this WP save those that are organized as joint events - to the level and in the format agreed with the corresponding co-host, shall be organized by the Secretariat. Unless agreed otherwise, the events shall take place in the premises of the Secretariat in Vienna.

Unless it is otherwise agreed and organized by the Secretariat in cooperation with a relevant donor / provider of technical assistance, and approved by the CyberCG, hosting of the exchange of electronic data related to the Activities of the Work Plans under 2), 3) and 4) shall be provided and organized by the Secretariat. For the hosting services provided by the Secretariat. The Energy Community Rules for Reimbursement[9] shall apply.

TIMELINE

The activities shall be performed according to the tentative schedule provided in Table 1.

[9] *Reimbursement Rules*

Table 1 – EnC CyberCG Work Plan 2020 - 2021

Tasks	Targets / Activities	2020												2021											
		Q1			Q2			Q3			Q4			Q1			Q2			Q3			Q4		
WG on ENERGY COMMUNITY CRITICAL INFRASTRUCTURES																									
I – ENERGY COMMUNITY CRITICAL INFRASTRUCTURES (WG-ECCI)	***1.1 Report on the status of Energy Critical Infrastructures / ES***	🟫	🟫	🟫	🟫																				
	- workshop on the Energy Critical Infrastructures / ES [CyberCG]				⬛																				
	1.2 Common platform for regional designation of ECCI	🟫	🟫	🟫	🟫	🟫	🟫																		
	- workshop on ECCI Designation Rules and Action Plan [CyberCG]						⬛																		
	2.1 Guidelines for OSP - Operator Security Plans					🟫	🟫	🟫	🟫	🟫															
	- TA on Operator Security Plans (OSP) drafting Methodology [ECS]							🟩	🟩	🟩															
	- training workshops on OSP Methodology / Guidelines [CyberCG]									🟧															
	2.2 Regional Implementation of Operator Security Plans										🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫
	- TA on regional Risk Analysis Methodology [ECS]										🟩	🟩	🟩												
	- workshop on the regional risk analysis Methodology [CyberCG]												⬛												
	- development / adoption of guidelines on regional risk analysis													▒	▒	▒	▒	▒	▒						
	- training on regional cyber threats / OSP exercise [CyberCG]																		🟧						
	- regional mechanisms for ECCI resilience support																			▒	▒	▒	▒	▒	▒
	- workshop on the regional ECCI resilience support [CyberCG]																								⬛
WG on CYBERSECURITY GOVERNANCE IN THE ENERGY COMMUNITY																									
II – CUBERSECURITY GOVERNANCE (WG-CG)	***3.1 Adaptation of the ECI Directive for the Energy Community***	🟫	🟫	🟫	🟫	🟫	🟫																		
	- workshop on the legal transposition of the ECI Directive [CyberCG]						⬛																		
	3.2 Adaptation of the NIS Directive for the Energy Community	🟫	🟫	🟫	🟫	🟫	🟫																		
	- workshop on the legal transposition of the NIS Directive [CyberCG]						⬛																		
	- adoption / application of ECI and NIS Directives in the EnC CPs							▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒	▒
	- Guidelines for implementation of cybersecurity acquis							🟫	🟫	🟫	🟫	🟫	🟫												
	- workshop - application of cybersecurity acquis in energy [CyberCG]												🟧												
	4.1 Report on the current Cybersecurity Strategies in energy													🟫	🟫	🟫	🟫								
	- technical workshop – presentation of Strategies Report [CyberCG]																⬛								
	4.2 Cybersecurity Strategy of the Energy Community													🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫
	- common cybersecurity planning methodology													▒	▒	▒	▒								
	- workshop on cybersecurity planning methodology [CyberCG]																⬛								
	- draft regional cybersecurity strategy																	▒	▒	▒	▒	▒	▒	▒	▒
	- training workshop on regional cybersecurity planning [CyberCG]																								🟧
	5.1 Cybersecurity in certification and tendering of new infrastructure	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫													
	- TA on methodology for minimum cybersecurity criteria [ECS, ECRB]			🟩	🟩	🟩																			
	- workshop on the cybersecurity conditions in tendering [CyberCG, ECRB]					⬛																			
	5.2 Cybersecurity in regulated prices and tariffs	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫													
	- TA on methodology for cybersecurity costs in tariffs [ECS, ECRB]			🟩	🟩	🟩																			
	- workshop on methodology for cybersecurity costs [CyberCG, ECRB]					⬛																			
	- guidelines on cybersecurity criteria for new infrastructure [ECS, ECRB]						▒	▒	▒	▒	▒	▒													
	- training on regulatory treatment of cybersecurity costs [CyberCG, ECRB]											🟧													
	5.3 Application of ISO 27000 standards in the Energy Community									🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	🟫	
	- TA on methodology and cost-benefit criteria for 27K [ECS, ECRB]													🟩	🟩	🟩									
	- workshop on ISO 27K methodology [CyberCG, ECRB]															⬛									
	- guidelines for technical standards on cybersecurity [ECS, ECRB]																▒	▒	▒	▒	▒	▒	▒	▒	
	- training on technical standards in cybersecurity [CyberCG, ECRB]																							🟧	

Tasks	Targets / Activities	2020												2021											
		Q1			Q2			Q3			Q4			Q1			Q2			Q3			Q4		
ENERGY COMMUNITY CYBERSECURITY NETWORKS																									
III – ENERGY COMMUNITY CSIRT[10] NETWORK	***6.1 EnC - CSIRTs electronic platform (setup)***	■	■	■	■	■																			
	- concept for operation, technical set-up, ToR, rules of procedure	▨	▨	▨	▨																				
	- SW installation and trial operation [ECS]				🟩	🟩																			
	- workshop on the EnC CSIRT communication platform [CSIRT WG]					●																			
	6.2 CSIRT Panel for Cybersecurity Cooperation (setup)			■	■	■	■	■	■	■	■	■	■	■	■										
	- methodology for regional risk criteria and risk assessment			▨	▨	▨	▨	▨																	
	- rules / protocol for real-time exchange of information / support					▨	▨	▨	▨	▨															
	- workshop on the mechanism for real-time assistance (CSIRT WG]									●															
	- application of the CSIRT panel protocol – test period									▨	▨	▨	▨	▨	▨										
	- training exercise on emergency data exchange [CSIRT WG]														●										
	6.3 CSIRT Panel for Planning and Education (setup)	■	■	■	■																				
	- rules / protocol for cooperation in the planning activities	▨	▨	▨	▨																				
	- program for education and training / action plan (ECS, WG)			▨	▨																				
	- workshop on CSIRT planning / education activities [CSIRT WG]				●																				
	6.4 Establishment of Energy Community Energy CSIRT	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
	- establishment / nomination of national energy CSIRT structures	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨														
	- draft rules / protocol and program for a regional energy CSIRT						▨	▨	▨	▨	▨														
	- workshop on the regional E-CSIRT mode of cooperation [CSIRT WG]										●														
	- follow-up on the establishment of EnC energy CSIRT											▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
IV – ENERGY COMMUNITY ENERGY ISAC[11]	***7.1 Establishment of Energy Community Energy ISAC***	■	■	■	■	■	■	■	■	■	■														
	- conference on PPP and cooperation in cybersecurity [CyberCG]				🟧																				
	- rules / protocol for cooperation of energy enterprises					▨	▨	▨	▨	▨	▨														
	- program for operation of EnC E-ISAC								▨	▨	▨														
	- TA on electronic platform for the EnC E-ISAC [ECS]									🟩	🟩														
	- workshop on establishment of EnC E-ISAC [CyberCG]										●														
	- follow-up activities of consultation activities											▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
	7.2 Platform for support in certification											■	■	■	■	■	■								
	- guidelines on certification criteria and policy [ECS, ENISA]											▨	▨	▨	▨										
	- rules / protocol for support to certification in energy														▨	▨	▨								
	- workshop / conference on certification in the energy sector																🟧								

[10] *Computer Security Incidents Response Team*

[11] *Information Sharing and Analysis Centre*

Tasks	Targets / Activities	2020												2021											
		Q1			Q2			Q3			Q4			Q1			Q2			Q3			Q4		
CyberCG EVENTS																									
PERIODIC EVENTS	*- CyberCG plenary meetings*						■						■						■						■
	- CyberCG public events				🟧					🟧							🟧					🟧			
CYBERSECURITY ACADEMY																									
EDUCATION AND TRAINING PROGRAM	*- workshop on the Energy Critical Infrastructures / ES [CyberCG]*				■																				
	- workshop on CSIRT planning / education activities [CSIRT WG]				■																				
	- conference on PPP and cooperation in cybersecurity [CyberCG]				🟧																				
	- TA on methodology for minimum cybersecurity criteria [ECS, ECRB]			🟩	🟩	🟩																			
	- workshop on the cybersecurity conditions in tendering [CyberCG, ECRB]					■																			
	- TA on methodology for cybersecurity costs in tariffs [ECS, ECRB]			🟩	🟩	🟩																			
	- workshop on methodology for cybersecurity costs [CyberCG, ECRB]					■																			
	- SW installation and trial operation [ECS, TA]				🟩	🟩																			
	- workshop on the EnC CSIRT communication platform [CSIRT WG]					■																			
	- workshop on ECCI Designation Rules and Action Plan [CyberCG]						■																		
	- workshop on the legal transposition of the ECI Directive [CyberCG]						■																		
	- workshop on the legal transposition of the NIS Directive [CyberCG]						■																		
	- TA on Operator Security Plans (OSP) drafting Methodology [ECS]							🟩	🟩	🟩															
	- training workshops on OSP Methodology / Guidelines [CyberCG]									🟧															
	- workshop on the mechanism for real-time assistance (CSIRT WG]									■															
	- TA on electronic platform for the EnC E-ISAC									🟩	🟩														
	- workshop on establishment of EnC E-ISAC										■														
	- workshop on the regional E-CSIRT mode of cooperation [CSIRT WG]										■														
	- training on regulatory treatment of cybersecurity costs [CyberCG, ECRB]											🟧													
	- TA on regional Risk Analysis Methodology [ECS]										🟩	🟩	🟩												
	- workshop on the regional risk analysis Methodology [CyberCG]												■												
	- workshop - application of cybersecurity acquis in energy [CyberCG]												🟧												
	- training exercise on emergency data exchange [CSIRT WG]														■										
	- TA on methodology and cost-benefit criteria for 27K [ECS, ECRB]													🟩	🟩	🟩									
	- workshop on ISO 27K methodology [CyberCG, ECRB]															■									
	- technical workshop – presentation of Strategies Report [CyberCG]																■								
	- workshop on cybersecurity planning methodology [CyberCG]																■								
	- workshop / conference on certification in the energy sector																🟧								
	- training on regional cyber threats / OSP exercise [CyberCG]																		🟧						
	- training on technical standards in cybersecurity [CyberCG, ECRB]																							🟧	
	- workshop on the regional ECCI resilience support [CyberCG]																								■
	- training workshop on regional cybersecurity planning [CyberCG]																								🟧
CO-ORGANIZATION OF EVENTS (proposal)	*- conference on smart energy networks / services and cybersecurity*					▨	▨	▨			▨	▨													
	- workshop on cybersecurity in the gas infrastructure			▨		▨	▨	▨			▨	▨													
	- workshop on energy production / storage and cybersecurity			▨		▨	▨	▨			▨	▨													
	- workshop on confidentiality of data in cybersecurity in energy										▨	▨			▨	▨		▨		▨					
	- conference on new technologies and cybersecurity										▨				▨	▨		▨		▨		▨	▨		

ANNEX 2

Working Group on Energy Community Critical Infrastructures WORK PLAN 2020 - 2021

The CyberCG established a working group on Energy Community Critical Infrastructures (**WG-ECCI**) following Items 1 and 5 of the CyberCG Terms of Reference[12] and Point 8 of the Conclusions[13] from the First CyberCG Meting of 11 April 2019.

COMPOSITION

The CyberCG Working Group on Energy Community Critical Infrastructures consists of the representatives from participating Parties which bear responsibility for identification and nomination of critical infrastructures in energy (Energy Ministry, NRA, liaison officers / official representatives from the operators of critical infrastructure), and ECS. The activities / meetings may include participants from ENISA, ACER, ECRB, ENTSO-E, ENTSOG and invited experts. To the extent the Programme involves regulatory aspects and/or the need for knowledge building of regulators in the context of cybersecurity, the CyberCG Working Group will involve the ECRB Section at the Secretariat, the ECRB President and ECRB Vice-Presidency as well as the chairpersons of the ECRB working groups.

DESCRIPTION

The overall target of WG-ECCI is to support (early) implementation of the obligations from the Directive 2008/114/EC[14] on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (**ECI Directive**), applicable to the energy sector and adapted to the Energy Community environment.

The ECI Directive, together with the following Items of Paragraph 2 of the CyberCG Terms of Reference define the energy domain of relevance for implementation of the Directive and corresponding WG activities:

(i) (d) '**operator of essential services**' means a public or private entity which provides an energy service that

a) is essential for the maintenance of critical societal and/or economic activities,
b) the provision of that service depends on network and information systems, and
c) 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 the NIS Directive[15].

(ii) (e) '**energy services**' comprise:

[12] https://www.energy-community.org/dam/jcr:a9163c92-fb05-40c3-a74c-acca91fe94c1/PA_02_2018_MC-EnC_CSCG_112018.pdf

[13] *https://www.energy-community.org/dam/jcr:6c7071f9-cc87-463d-9dcd-26604036936c/CyberCG_Conclusions_052019.pdf*

[14] *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN*

[15] *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN*

- electricity generation, supply, market operation, distribution, transmission and storage;
- natural gas production, supply, market operation, transmission, distribution, storage and LNG;
- oil production, refining and treatment facilities, market operation, storage and transmission;
- monitoring and control of pollution and emissions from energy combustion, and
- 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.

(iii) (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;

(iv) (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;

The reference to "essential services" in item (i) is not generic for the ECI Directive (it has been introduced in this context in 2016, by the NIS Directive[16]) however due to its relevance for cybersecurity, for the purpose of the WB ECCI activities and this Plan it shall implicitly complement the scope of the definition of critical infrastructures. Additionally, the definitions of the ECI Directive apply.

Notwithstanding possible interest for participation of stakeholders from the other fields, the Group shall in the first place follow the scope of energy sectors identified in *Annex I* of the Directive – electricity, oil and gas.

ECI Directive is not yet mandatory for the Energy Community – its implementation is supported by the PHLG in the form of recommendation as acquis of relevance for Energy Community, and its adaptation for legal transposition is a subject of consideration by the WG on Governance.

The energy sector is one of high relevance with respect to ECI Directive considerations, with high level of critical infrastructures and specific security requirements. Such requirements are real-time protection of the continuous operation, prevention of possible cascading disruptions (both through the energy and information channels), and application of mixed technologies (both legacy / analogue, and digital) – as identified in the Commission Recommendation[17] on cybersecurity in the energy sector.

[16] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[17] https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf

The energy systems are of vast and critical importance for the economy and bear ultimate social value, which makes their protection a matter of highest priority in each country. Furthermore the energy policies change, systems develop and the applied technologies evolve, which makes the process for identification, designation and protection of critical infrastructures continuous – calling for the establishment of mechanisms capable for sustained protection in the security domain. All of that implies the need for close cooperation among different sectors and institutions in the country and engagement of significant human and financial resources.

The energy networks are highly interconnected (on regional and pan-European level) building up the possibility a security threat in the infrastructure of one country critically affecting the security conditions in a systems across its borders. ECI Directive regulates the need for designation of critical infrastructure in such cases, which calls for coordination and sustained cooperation on regional level in this domain.

The ECI Directive defines and treats the security of the critical energy infrastructure in a generic manner, not focusing only on cybersecurity. That approach shall be sustained in the basic aspects of implementation as much as applicable – in the analysis, administrative procedures, authorities and bodies, their responsibilities, in the policy domain, proposed cooperation measures and mechanisms, etc. (which may have a broader scope of security references). The risk-related aspects – assessment criteria, methodology, and requirements for the protection measures, shall focus on the specific cybersecurity domain, which shall have impact on the identification of ECI and on the security plans.

SCOPE OF ACTIVITY

TASK 1 – Identification and designation of critical energy infrastructures

The Group will cooperate and endeavour in achievement of the following targets:

1.1 **Target I** – **Review / report on the current state of CI / ES**

Conduct a review and develop a Report on the current state of identification / designation of critical infrastructures and related ongoing developments, on national grounds.

The Report will include (as its minimum):

(i) the legal / administrative environment for identification of critical energy infrastructures, responsible bodies,

(ii) state of development / adoption / publication of rules, criteria and procedures for identification of critical energy infrastructures, adopted plans and deadlines for future activities;

(iii) cases (list) of identified energy infrastructures / appointed liaison officers (all relevant energy domains according to the CyberCG Terms of Reference - Item 2(e);

(iv) mechanisms / agreements for cross-border designation and cases (list) of bilaterally or multilaterally designated critical infrastructures.

The data collection / stocktaking activities shall be done by the national representatives, under responsibility of the focal points, assisted by ECS. Finalization of the document shall be done by ECS. The final Report shall be discussed and adopted by the WG-ECCI and presented to CyberCG. CyberCG shall decide on its publication.

Deliverables:

- ❖ a Report on the state of affairs in the identification and designation of critical energy infrastructures; the Report shall be consulted with ECRB as regards recognition of related costs in the regulatory tariff.
- ❖ Workshop for the CyberCG on the findings with presentation on national level and discussion, comparable reference with EU and other domains -– press release, publication. The WS should include the activities of the CyberCG WG-CG (Target I) on the transposition of the ECI Directive.

Preconditions:

- available information / access to data on national level – no confidentiality issues, administrative barriers, cooperation of enterprises;
- Cooperation with the CyberCG WG-CG on the related Task for transposition of the consolidated Directive;

Timing:

- tentative duration of the activity is **4 months**. The WS to be organized back-to-back with a CyberCG meeting.

Estimated cost:

- [EUR] (costs of a WS)

1.2 Target II – Common platform for regional designation of ECCI

Develop a common platform (set of rules and mechanisms) for identification of CI on national level, and designation of ECCI on bilateral / multilateral level on the territories of the Energy Community Contracting Parties and EU Member States of the Title III of the Energy Community treaty.

The activity will include the following steps:

(i) Identify / adopt a set of minimum coordinated criteria for identification and for designation of critical energy infrastructures in the relevant domains (electricity, gas, oil) on Energy Community / WG level; the set of minimum criteria shall be consulted with ECRB

(ii) Develop / adopt rules for exchange / protection of confidential information referring to critical energy infrastructures;

(iii) Define possible coordinated bilateral / multilateral procedure(s) for designation of critical energy infrastructures applicable among the concerned countries – the measure should be applied in a continuous / revolving format;

(iv) Develop / adopt / apply a common mechanism for monitoring / reporting in the process of identification / designation of critical energy infrastructure,

(v) Develop and adopt an Action Plan along with an instrument for legal / political enforcement (MoU / MC decision / PA) of the cooperation in the designation of critical energy infrastructures including a common programme with deadlines / targets (related to existing energy infrastructure and one to be commissioned before the targeted deadlines), propose it for enforcement in the Energy Community;

A general framework for the procedure of Item (iii) is provided in the Annex III of the ECI Directive.

The work shall be done by national representatives under responsibility of the focal points and supported by ECS. Initial drafts for items (i), (iii) and (v) shall be proposed by ECS. The mechanisms under (i), (ii), (iii) and (iv) shall be integrated in a common act (Rules) adopted by the CyberCG, approved by the NRA and implemented through (v). The final format of the documents shall be consolidated by ECS. ECS shall provide support in drafting the proposal and in the procedure for adoption by the EnC governance body of the enforcement instrument (v).

Deliverables:

- ❖ Common Rules for identification and designation of ECCI - Energy Community Critical Infrastructures in energy;
- ❖ Action plan for identification and designation of ECCI;
- ❖ Instrument for enforcement of the minimum required cooperation between the Interested Parties in the implementation of the Action Plan.
- ❖ Workshop for the CyberCG on the Rules and Action Plan – discussion, comparable reference with EU and other domains – press release, publication.

Preconditions:

- Cooperation / agreement between responsible authorities / NRA in support of the coordinated approach, minimum set of relevant criteria which can be coordinated with foreign authorities;
- elimination of legal / political obstacles for implementation of an international cooperation mechanism, Parties willing to enter into a common mechanism, relevant EnC governance bodies (MC, PHLG) agreed on the common platform and targets;

Timing:

- tentative duration of the whole activity is **6 months**. Task 1 is not a prerequisite – both tasks could be implemented in parallel. The WS to be organized back-to-back with a CyberCG meeting.

Estimated cost:

- [EUR] (costs of a WS)

TASK 2 – Operator Security Plans (OSP)

The Group will cooperate and endeavour in achievement of the following targets:

2.1 **Target III** – **Guidelines for Operator Security Plans**

Develop and adopt guidelines for establishment of Operator Security Plans (OSP) on national level including a platform for coordinated OSP in the cases of bilaterally and multilaterally designated critical infrastructures.

The activity will include the following steps:

(i) Provide a (provisional) review of existing security plans, risk-assessment exercises and corresponding applied protection measures; provide a review of appointed liaison officers and their responsibilities / competences / legal enforcement;

(ii) Adopt a reference set of criteria and threat scenarios for security / cybersecurity risk assessment – for national level and regional level;

(iii) Adopt a set of criteria and general conditions for appraisal of possible security solutions / measures, relative to the level of risk / type of infrastructure / security environment;

(iv) Develop methodologies for implementation of bilateral / multilateral security measures for the designated CI, for joint security verification exercises following specific threat scenarios, for joint supervisory / oversight arrangements and for reporting;

(v) Develop / adopt consolidated Guidelines for the Operator Security Plans which among else, integrate items (i) through (iv); ensure compliance of the guidelines and their approval on national level (NRA);

(vi) Prepare / adopt an instrument for enforcement of the Guidelines by relevant EnC authority (MC / PHLG) and propose it for adoption.

A general framework for developing the OSP is provided in Paragraph 5 and Annex II of the ECI Directive.

The work shall be done by national representatives under responsibility of the focal points and supported by ECS. The review of Item (i) could be completed in the scope of reporting results of Target I. Initial drafts for items (iv), (v) and (vi) shall be proposed by ECS. All the criteria and methodologies under (ii), (iii) and (iv) shall be integrated in the consolidated Guidelines of Item (v), adopted by the CyberCG, approved by the NRA and enforced through (vi). The final format of the documents shall be consolidated by ECS. ECS shall also provide support in designing the proposal and in the procedure for adoption by the EnC governance body of the enforcement instrument (vi). Technical assistance is planned on the OSP Drafting Methodology (guidelines / templates).

Deliverables:

- ❖ Report on existing / applied security plans, risk-assessment results and protection measures for critical energy infrastructure in the Energy Community; the Report shall be consulted with ECRB
- ❖ Report on appointed liaison officers for critical energy infrastructure in the Energy Community;
- ❖ Guidelines for establishment and implementation of Operator Security Plans (OPS) for critical energy infrastructures in the Energy Community;
- ❖ Workshop (training) for the CyberCG on the Guidelines – discussion, comparable reference with EU -– press release, publication.

Preconditions:

- The Reports have the same preconditions as Target I;
- The activities in (ii), (iii), (iv) and (v) have the same preconditions as Target II. Additionally the participation of stakeholders for specific types of infrastructure requires such infrastructures to be already identified / designated;

Timing:

- tentative duration of the whole activity is **5 months**. The WS to be organized back-to-back with a CyberCG meeting.
- the activities need significant engagement / participation from stakeholders of already designated CI on regional level – activities should come later than Target 1, aligned with the Action Plan of Target 2.

Estimated cost:

- [EUR] (costs of a WS)
- [EUR] (costs of TA for the Methodology) – 10 expert days

2.2 **Target IV – Regional Implementation of Operator Security Plans**

Develop, adopt, apply and monitor an Action Plan, with timing and targets, for development / implementation of the Operator Security Plans, appointment of liaison officers and performed regional cyber threat simulation exercises, on national and Energy Community level.

The activity will include the following steps:

(i) Develop a methodology for oversight of the implementation of OSP along with the criteria for monitoring and reporting to CyberCG on of the pace of development / implementation of the Operator Security Plans;

(ii) Develop and adopt a methodology for regional cyber threat exercise and regional Risk Analysis according to specific scenarios;

(iii) Develop and adopt a consolidated Action Plan for implementation of OPS on national and Energy Community level, including the methodologies, applicable to already identified and/or bilaterally / multilaterally designated critical infrastructures, with timing and targets; including a mechanism for oversight and reporting on Energy Community level;

(iv) Ensure compliance of the methodologies and the Action Plan and their approval on national level (by NRA);

(v) Prepare / adopt an instrument for enforcement of the Action Plan by relevant EnC authority (MC / PHLG) and propose it for adoption.

The work shall be done by national representatives under responsibility of the focal points and supported by ECS. Initial drafts for the Items (i), (iii) and (v) shall be provided by ECS, as well as the consolidated Action Plan and the final documents of Item (v). The development of the methodology of Item (ii) may need outsourcing (engagement of expert consultants) and cooperation with EU authorities (EC, ENISA, ACER) for transfer of best practices. Technical assistance is foreseen on development of a regional Risk Analysis Methodology.

Deliverables:

- ❖ Action Plan on the implementation of Operator Security Plans (OSP) in the Energy Community – including timing and targets, as well as monitoring and reporting mechanism;
- ❖ Methodology for regional Risk Assessment (guidelines);
- ❖ Workshop for the CyberCG on the Methodology – discussion, comparable reference with EU and other domains – press release, publication.
- ❖ Training workshop on regional cyber threats and exercises on OSP application
- ❖ Guidelines / regional mechanism for ECCI resilience support
- ❖ Workshop on the ECCI resilience - regional support

Preconditions:

- The development of the methodologies and draft Action Plan and their approval – Items (i), (ii), (iii) and (iv) have the same preconditions as Target II;

- For the application of the Monitoring and Reporting activities and the overall Action Plan the critical infrastructures has to be already identified / designated and the Guidelines for OSP of Target III to be adopted and applied.

Timing:

- tentative duration of the overall activity is **15 months**. The implementation, monitoring and reporting shall have continuous / revolving time pattern. The WS to be organized back-to-back with a CyberCG meeting.
- activities should commence later than Target 1, aligned with the Action Plan of Target 2.

Estimated cost:

- [EUR] (costs of 3 WS events)
- [EUR] (costs of a TA for the Methodology of Item (ii)) – 15 expert days

ANNEX 3

Working Group on Cybersecurity Governance
WORK PLAN 2020 - 2021

The CyberCG established a working group on Cybersecurity Governance (WG-CG) following Items 1 and 5 of the CyberCG Terms of Reference[18] and Point 9 of the Conclusions[19] from the First CyberCG Meting of 11 April 2019.

COMPOSITION

The CyberCG Working Group on Cybersecurity Governance consists of the representatives of participating Parties from the authorities responsible for the legal and regulatory framework in the domains of energy security and cybersecurity, and on application of cybersecurity-related technical standards – the Ministries responsible for energy and for information technology, NRAs, and ECS. The activities / meetings may include participation of EC, ENISA, ACER, ECRB, ENTSO-E, ENTSOG and invited experts.

DESCRIPTION

Main target of the WG-CG is coordination in the development of comprehensive legal and regulatory frameworks for cybersecurity in the Energy Community Contracting Parties compliant with the EU acquis.

Main acts for consideration include, but are not limited to:

(i) Council Directive[20] 2008/114/EC on the identification and designation of European critical infrastructures and assessment of the need to improve their protection – the **ECI Directive**;

(ii) Directive[21] (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union – the **NIS Directive**;

(iii) Directive[22] 2002/21/EC on a common regulatory framework for electronic communications networks and services;

(iv) Regulation[23] (EU) 2019/941 on risk preparedness in the electricity sector;

(v) Regulation[24] (EU) 2017/1938 concerning measures to safeguard the security of gas supply;

[18] https://www.energy-community.org/dam/jcr:a9163c92-fb05-40c3-a74c-acca91fe94c1/PA_02_2018_MC-EnC_CSCG_112018.pdf

[19] *https://www.energy-community.org/dam/jcr:6c7071f9-cc87-463d-9dcd-26604036936c/CyberCG_Conclusions_052019.pdf*

[20] *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN*

[21] *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN*

[22] *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0021&from=en*

[23] *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0941&from=EN*

[24] *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R1938&from=EN*

(vi) Standard series[25] **ISO 27000** (27001, 27002, 27005, 27032 and eventual other parts which are considered relevant for the energy sector),

and other acts that shall be included on a later date.

The provided list is indicative even for the ongoing two-year term (2020 – 2021). It shall be modified and complemented through Decisions taken by CyberCG, upon a proposal from ECS supported by the WG-CG. Other legal / regulatory acts that may be tentatively considered / processed by the WG include: a new EU network code and guidelines on cybersecurity, EC recommendations on cybersecurity in energy, future ENTSO-E / ENTSOG acts in this area, other acquis that appears directly or indirectly relevant, other technical standards, etc.

Most of the legal matter at hand typically addresses a broader domain of cybersecurity-related activities in other sectors beside energy (transport, communications, data protection, banking, health, etc.). Some legal acts (acquis) with its primary governance domain in sectors other than energy and/or cybersecurity (e.g. environment) may contain provisions relevant for enhancing cybersecurity in energy. In such cases only those provisions (titles, chapters, paragraphs, technical rules), or corresponding legal / regulatory matter, which are:

a) relevant (directly or indirectly) for cybersecurity in the energy sector – in provision of energy services, and
b) applicable by the Energy Community Contracting Parties;

shall be taken into consideration, processed, consolidated and promoted to EnC authorities for adoption.

Looking at the energy sector, a more specific list of the energy services considered relevant for cybersecurity is provided in the item 2(e) of the CyberCG ToR, including:

- electricity generation, supply, market operation, distribution, transmission and storage;
- natural gas production, supply, market operation, transmission, distribution, storage and LNG;
- oil production, refining and treatment facilities, market operation, storage and transmission;
- monitoring and control of pollution and emissions from energy combustion, and
- 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.

Related to the cybersecurity relevant acquis, the targets of the WG-CG shall be in development, adjustment and adoption by the CyberCG of an adapted version of the legal act which is in compliance with the acquis and compatible with the above two restrictions. Such a common act shall be proposed for adoption by the Energy Community governance bodies (Ministerial Council, PHLG or ECRB).

The proposed draft acts shall include adjustments and/or extension of the original act, as agreed by the WG, stemming from related, more recent EU / EC legal acts, recommendations, implementation notes, clarifications, policy documents and best practices, or from other EU acquis which is considered substantial for the subject matter. ECS shall consolidate the adjusted version and propose it for discussion and agreement.

[25] https://www.iso.org/isoiec-27001-information-security.html

In the process, the WG shall typically apply two rounds of external consultations (in addition to possible external technical assistance eventually engaged) – with the main national operators of critical infrastructure / providers of essential services (in consultation of the draft text during its development), and with the national energy / cybersecurity authorities (for official approval of the final draft before its submission for adoption by the EnC authorities).

Transposition in the national legislation and adoption by the Contracting Parties shall be conducted according to national practices of each country. The act may be transposed in an integral or fragmented form (e.g. in case parts are already enforced), in one or more acts, in legal acts or governmental / regulatory rules. ECS shall monitor / support the process of adoption and asses the compliance, the Contracting Parties shall report their progress to the CyberCG.

In addition to the normative acts (laws / regulations) the cybersecurity governance domain of interest also includes technical standards and policy acts.

The main set of technical standards relevant for cybersecurity are the ISO 27000 series, addressing several domains of corporate organization and operation. Main authority responsible for application of the standards should be the NRA. The overall scope of security aspects covered by the standards may exceed the cybersecurity needs – which depend on the type and size of the enterprise, and eventually the available funds. In that context the WG shall target development of criteria and recommendations on the patterns of standards and modes of their application for various types of stakeholders, and sharing of best practices.

The obligation for adoption of a cybersecurity strategy on national level is stemming from the NIS Directive (Article 7). Notwithstanding the efforts of national authorities and results in that direction, the CyberCG WG should engage on consolidation of the cross-border aspects in the domain of strategic planning, the cooperation requirements and on streamlining the development of required mechanisms on regional level.

SCOPE OF ACTIVITY

TASK 3 – EU acquis on cybersecurity for adoption in the Energy Community

The Group will cooperate and endeavour in achievement of the following targets:

3.1 Target I – Adaptation of the ECI Directive for the Energy Community

Develop and adopt an adjusted version of the **ECI Directive**[26] to be applied in the energy sector, and prepare its submission tor enforcement through the Energy Community governance bodies – to be adopted in the format of minimum mandatory legal framework, and implemented at national level.

The activity will include the following steps:

(i) Identify the set of articles (the legal matter) of ECI Directive relevant for the energy sector, which should be mandatory for implementation. Provide a review of the state of transposition of the ECI Directive in the mandatory format by the Contracting Parties;

[26] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

(ii) Develop an adjusted version of the legal matter from the ECI Directive including the provisions relevant for the energy sector, with the parts most relevant for cybersecurity in energy expanded / complemented by provisions from corresponding acquis, and other (more recent) EU acts or documents regulating the subject matter as described before;

(iii) Conduct consultation with the stakeholders - operators of CI and providers of essential services (as indicated in the NIS Directive), NRA and ministries responsible for energy and for cybersecurity;

(iv) Prepare the final consolidated version of the legal text and propose to CyberCG for adoption, along with the instrument for enforcement – adoption by the Energy Community governance bodies (PHLG, Ministerial Council);'

(v) Prepare and propose to CyberCG for adoption an Action Plan with deadlines for transposition and implementation of the ECI Directive, and criteria for assessment of compliance, monitoring and reporting.

The analytic work and the comments / proposals shall be done by national representatives under responsibility of the focal points and supported by ECS. Initial drafts for the Items (ii), and (iv) shall be provided by ECS, as well as the draft for the Action Plan of Item (v). The CyberCG WG-CG representatives shall provide the review in item (i) and conduct the consultations of Item (iii) for each individual Party.

The (early) implementation of the Directive has been defined as a separate task for another WG – the CyberCG WG-ECCI. Both Working Groups shall closely cooperate and complement their activities. The developments shall be addressed in the workshop for Target I of that Group.

Deliverables:

- ❖ Adjusted version of the **ECI Directive** to be transposed and adopted by the CPs; the adjusted version shall be consulted with ECRB
- ❖ Action plan for transposition and implementation of the adapted ECI Directive with criteria for compliance

Preconditions:

- The level of already achieved transposition of the ECI Directive in the CPs – the findings may influence the contents of the proposal;
- Cooperation with the CyberCG WG-ECCI on the related Task for early implementation of the Directive;

Timing:

- tentative duration of the overall activity is **6 months**. The consequent transposition, adoption and implementation by CPs shall require continuous monitoring / reporting.
- activities should commence in parallel with Target 1 of the WG ECCI.

Estimated cost:

- NO specific cost is foreseen for this Target.

3.2 Target II – Adaptation of the NIS Directive for the Energy Community

Develop and adopt an adjusted version of the **NIS Directive**[27] to be applied in the energy sector, and prepare its submission tor enforcement through the Energy Community governance bodies – to be adopted in the format of minimum mandatory legal framework, and implemented at national level.

The activity will include the following steps:

(i) Identify the set of articles (the legal matter) of NIS Directive relevant for the energy sector, which should be mandatory for implementation. Provide a review of the state of transposition of the NIS Directive in the mandatory format by the Contracting Parties;

(ii) Develop an adjusted version of the legal matter from the NIS Directive including the provisions relevant for the energy sector, with the parts most relevant for cybersecurity in energy expanded / complemented by provisions from corresponding acquis, and other (more recent) EU acts or documents regulating the subject matter as described before;

(iii) Conduct consultation with the stakeholders - operators of critical infrastructures and providers of essential services, CSIRTs, NRA and ministries responsible for energy and for cybersecurity;

(iv) Prepare the final consolidated version of the legal text and propose to CyberCG for adoption, along with the instrument for enforcement – adoption by the Energy Community governance bodies (PHLG, Ministerial Council);'

(v) Prepare and propose to CyberCG for adoption an Action Plan with deadlines for transposition and implementation of the NIS Directive, and criteria for assessment of compliance, monitoring and reporting.

(vi) Develop and propose to CyberCG for adoption Guidelines / Recommendations for implementation of the NIS Directive and other AU acquis / recommendations applicable in energy, based on the EU best practices – in the form of a policy paper. Prepare a procedure for transposition and implementation of new acquis on cybersecurity in energy.

The analytic work and the comments / proposals shall be done by national representatives under responsibility of the focal points and supported by ECS. Initial drafts for the Items (i), (ii), (iv) and (vi) shall be provided by ECS, as well as the draft for the Action Plan of Item (v). The CyberCG WG-CG representatives shall provide the review in item (i) and conduct the consultations of Item (iii) for each individual Party.

Deliverables:

- ❖ Adjusted version of the **NIS Directive** to be transposed and adopted by the CPs;
- ❖ Action plan for transposition and implementation of the adapted NIS Directive with criteria for compliance;
- ❖ Workshop on the transposition of NIS directive in the energy sector;
- ❖ Recommendations (policy paper) for implementation of the NIS Directive.
- ❖ Workshop for the CyberCG on the Action Plan and Recommendations including the transposition of new acquis – discussion, comparable reference with EU and other domains – press release, publication.

[27] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Preconditions:

- Cooperation between authorities and stakeholders on national level from different sectors, each responsible for the implementation of NIS Directive in their domain;
- Cooperation between representatives and authorities from different Parties on the definition and implementation of legal provisions regulating activities on regional level;

Timing:

- tentative duration of the overall activity is **12 months**. The consequent transposition, adoption and implementation by CPs shall require continuous monitoring / reporting.

Estimated cost:

- [EUR] (costs of 2 WS)

TASK 4 – Energy Cybersecurity Strategies in the Energy Community

The Group will cooperate and endeavour in achievement of the following targets:

4.1 Target III – Report on the Cybersecurity Strategies of the Energy Community

Prepare a review and draft a Report on the energy context in the existing cybersecurity strategies and related acts, as well as the cybersecurity contents in the existing energy strategies and planning documents in the Energy Community Contracting Parties, including a compliance assessment and gap analysis with the Acquis. Develop and apply a set of criteria for the applicability appraisal on regional level and include a benchmark in the Report

The activity will include the following steps:

(i) Develop and adopt benchmark criteria and template for assessment of relevance / compliance / gap analysis of cybersecurity in the energy sector, for the existing strategic documents;

(ii) Provide a Review of existing national cybersecurity strategies and those drafts in development, (on the aspects relevant for the energy sector), and the national energy strategies and other acts aimed at implementing planning policies related to energy or energy infrastructure (on the aspects relevant for cybersecurity). Make assessment on compliance with the acquis and the EU cybersecurity policies and provide gap analysis and a benchmark review on regional level;

(iii) Conduct consultation on the findings with the national authorities for energy and cybersecurity (ministries, NRA, CSIRTs) and main stakeholders (operators of critical infrastructures and providers of essential services), and make adjustments as required;

(iv) Prepare a Report on the existing state of cybersecurity strategic planning in the energy sector ready for further gap analysis and consolidated approach;

The analytic work shall be done by ECS and the comments / proposals shall be done by national representatives under responsibility of the focal points and supported by ECS. Initial drafts for the Items (i) and (ii) shall be provided by ECS. The representatives shall provide comments on (i), support the collection of information for the review in item (ii) and conduct the consultations of Item (iii) for each individual Party. The Report shall be used as basis (precondition) for the Recommendations for updates on national level and the development of a Regional Cybersecurity Strategy of Target IV.

Deliverables:

- ❖ Report on the existing national cybersecurity strategies for the Energy Sector in the Energy Community, with compliance benchmark and gap analysis;
- ❖ Workshop for the CyberCG on the Report – discussion, press release, publication.

Preconditions:

- Access to existing strategies and other planning documents related to cybersecurity planning in the energy sector;
- Cooperation and support from the cybersecurity authorities and energy authorities / NRA on national level;

Timing:

- tentative duration of the overall activity is **4 months**. The consequent activities foresee development of consolidated regional cybersecurity strategy in the Energy Community as defined in Target IV.

Estimated cost:

- [EUR] (costs of a WS)

4.2 Target IV – Regional Cybersecurity Strategy of the Energy Community

Develop a methodology for regional strategic planning for cybersecurity in energy, perform gap analysis and consolidate the strategic acts on national level for cybersecurity in the energy sector, and adopt a Regional Cybersecurity Strategy for energy in the Energy Community.

The activity will include the following steps:

(i) Develop and adopt a methodology for cybersecurity planning with compliant, coordinated policy criteria and a set of (minimum) mandatory conditions and targets on national and regional level and conditions for coordinated timing, including a basic structure of key regional cooperation policies to be included in the regional strategy (including descriptions and SWOT analysis) and draft rules / procedures for regional coordination and enforcement;

(ii) Use the Report on the review / benchmark / gap analysis of the national cybersecurity strategies of Target III and the information / report on compliance with cybersecurity acquis of Target I as a source and develop / approve a set of minimum, (country-specific) proposals for update of the corresponding national cybersecurity strategies (or development of new ones) applicable in energy;

(iii) Develop draft regional Energy Cybersecurity Strategy for the Energy Community on regional level including regional mechanisms and policies, and Action Plan (roadmap) for coordinated implementation with timings and mechanisms for enforcement on national level;

(iv) Conduct consultation on the draft Strategy with the national authorities for energy and cybersecurity (ministries, NRAs, CSIRTs) and main stakeholders (operators of critical infrastructures and providers of essential services), and make adjustments;

(v) Prepare the final version of the Strategy along with an instrument for monitoring / reporting of its application and propose it to CyberCG for adoption.

(vi) Prepare an instrument for adoption by Energy Community Governance structure (PHLG, Ministerial Council) for its application in the Energy Community. Prepare and apply a mechanism for monitoring / reporting.

The analytic work, access to the required sources information and comments / proposals shall be provided by the national representatives under responsibility of the focal points and supported by ECS. Initial drafts for the Items (i), (ii), (iii) and (v) shall be provided by ECS. The representatives shall provide comments in item (i), (ii) and (iii), and conduct the consultations of Item (iii) for each individual Party.

Deliverables:

- ❖ Methodology for cybersecurity planning for the energy sector on national and regional level;
- ❖ Recommendations for complementary provisions (upgrades) of the national cybersecurity strategies;
- ❖ Workshop on the cybersecurity methodology
- ❖ A Regional Cybersecurity Strategy for the Energy Sector in the Energy Community, with Action Plan and Targets;
- ❖ Technical workshop for CyberCG on the methodology for coordinated and regional aspects of cybersecurity strategy;
- ❖ Workshop for the CyberCG and broader energy / cybersecurity community on the Regional Cybersecurity Strategy and cybersecurity planning – discussion, comparable reference with EU and other domains – press release, publication.

Preconditions:

- Cooperation between cybersecurity authorities / CSIRTs and energy authorities / NRA on national level;
- Flexibility / interest for coordination and adjustment of national policies / targets to regional requirements.

Timing:

- tentative duration of the overall activity is **12 months**. The consequent activities foresee continuous monitoring / reporting.

Estimated cost:

- [EUR] (costs of 2 WS)

TASK 5 – Regulatory treatment of Cybersecurity in energy

The Group will cooperate and endeavour in achievement of the following targets:

5.1 Target V – Cybersecurity in certification and tendering of new infrastructures

Develop and adopt coordinated Rules, including a Methodology and criteria for minimum compulsory cybersecurity requirements to be included in certification and tendering procedures and licenses for new energy infrastructures, along with corresponding framework for impact assessment.

The criteria and required measures shall address the cybersecurity risk associated with commissioning of new critical energy infrastructures in a Party, between Parties or within the interconnected network. The Rules shall also address general criteria for selection of technologies and certification requirements. The principle of a compulsory cybersecurity requirement shall relate to assessment of corresponding cybersecurity costs to be further estimated and included in the regulated prices or tariffs applied for public infrastructures.

The activity will include the following steps:

(i) Develop a draft Methodology for differential risk assessment for cases of commissioning new energy infrastructures with sensitivity analysis for different types / categories of infrastructure and different technologies;

(ii) Develop draft coordinated criteria for minimum compulsory cybersecurity preconditions and measures, relative to the type of infrastructure, technology, location and related type of service, aimed to be included as a preconditions in the criteria for certification, tendering and/or licensing of (new) energy infrastructure and/or essential services;

(iii) Develop draft framework criteria for impact assessment associated with the cybersecurity measures and preconditions of Item (ii);

(iv) Discuss the proposals of Items (i), (ii) and (iii) with NRAs via ECRB, Ministries, operators and relevant technology providers as applicable, and agree a common platform;

(v) Develop draft coordinated Rules for treatment of cybersecurity requirements in the procedures for (new) energy infrastructure certification and tendering, as well as licensing of (new) critical infrastructures and/or essential services, which shall include the agreed platform of Item (iv);

(vi) Prepare a final consolidated version of the Rules, reviewed and approved by the ECRB, and adopt the Rules.

The analytic work for the activities of Items (i), (ii), and (iii) shall be outsources and implemented through technical assistance (TA) of an expert team, which will provide the draft deliverables and corresponding information / training. The ToR for the TA shall be drafted by ECS. The comments / proposals related to these three Items shall be done by national representatives and NRA and other authorities responsible for commissioning energy infrastructures, as well as technology providers, operators and providers of essential services as applicable, under the responsibility of the focal points and ECRB and supported by ECS. Initial draft for the Item (v) shall be provided by ECS. The CyberCG WG-CG representatives and ECRB shall support the consultations for each individual Party.

The Methodology and the Rules shall be reviewed and approved by the ECRB.

Deliverables:

❖ Methodology for risk assessment and compulsory cybersecurity requirements for critical energy infrastructures and essential services;

- Rules for cybersecurity requirements in certification and tendering procedures and licenses for new energy infrastructures and essential services;
- Workshop for the CyberCG on the Methodology;
- Training session on the Methodology and the application of the Rules – discussion, comparable reference with EU, impact assessment criteria, enforcement criteria, etc. – press release, publication.

Preconditions:

- Agreement on the common approach in identification of minimum compulsory cybersecurity conditions
- Cooperation between cybersecurity authorities, energy stakeholders and NRA on national level;
- Technical assistance for developing the Methodology;

Timing:

- Tentative duration of the overall activity is **12 months**. Preferably, the same TA experts and the same TA timeframe shall be applied as in the corresponding activities of Target VI of this Task. The overall activity, as well as the workshops, ECRB engagement and the training session will be implemented in parallel with the ones in Target VI.

Estimated cost:

- [EUR] (costs of 2 WS)
- [EUR] (costs of a TA for the requirements of Item (ii)) – 12 expert – days;

5.2 Target VI – Cybersecurity costs in regulated prices and tariffs

Develop and adopt a Methodology for assessment of consolidated cybersecurity costs, to be calculated and applied as parts of regulated prices / tariffs, caused by implementation / application / operation of minimum compulsory cybersecurity technologies and measures associated with the use of critical energy infrastructures and essential services subject to regulated pricing. Criteria for identification of the compulsory cybersecurity measures are not included (defined separately).

The activity will include the following steps:

(i) Develop a draft general, coordinated methodology including criteria, procedure and conditions for estimation of costs resulting from the compulsory cybersecurity measures imposed on (new) energy critical infrastructures and essential services;

(ii) Develop draft Guidelines for implementation of the methodology and application of the costs in the pricing methodologies in the cases of regulated prices of essential services and/or connection fees and tariffs for access to critical energy infrastructures;

(iii) Discuss the draft Methodology and Guidelines of Items (i) and (ii) with NRAs via ECRB and operators as applicable, and agree on a common platform;

(iv) Prepare a final consolidated version of the Guidelines, including the Methodology, provide a review and approve it by the ECRB, and adopt the Guidelines.

(v) Develop and apply a mechanism for monitoring / reporting to CyberCG the application of the Guidelines and treatment of cybersecurity costs in the methodologies for regulated prices of energy / essential services and tariffs.

The analytic work for the activities of Items (i) and (ii) shall be outsources and implemented through technical assistance (TA) of an expert team, which will provide the draft deliverables and corresponding information / training. The ToR for the TA shall be drafted by ECS. The comments / proposals related to these two Items shall be done by national representatives and NRAs, as well as operators and providers of essential services as applicable, under the responsibility of the focal points and ECRB and supported by ECS. Initial drafts for the Items (ii) and (iv), and proposals for Item (v), shall be provided by ECS. The CyberCG WG-CG representatives and ECRB shall support the consultations for each individual Party.

The methodology and the Guidelines shall be reviewed and approved by the ECRB.

Deliverables:

- ❖ Methodology for assessment of cybersecurity costs to be applied as parts of regulated energy prices / tariffs;
- ❖ Guidelines for application of cybersecurity costs (cybersecurity criteria for new infrastructure) in the pricing methodologies for regulated prices and tariffs;
- ❖ Workshop for the CyberCG on the Methodology;
- ❖ Training session on the Methodology and the application of the Guidelines – discussion, comparable reference with EU, impact from the new technologies, effects on the energy market, enforcement criteria, etc. – press release, publication.

Preconditions:

- Agreement on the common approach in coordinated pricing methodology
- Cooperation between cybersecurity authorities, energy stakeholders and NRA on national level;
- Technical assistance for development of Methodology and draft Guidelines;

Timing:

- Tentative duration of the overall activity is **12 months**. Preferably, the same TA expert team and the same TA timeframe shall be applied as in the corresponding activities of Target V of this Task. The overall activity, as well as the workshops, ECRB engagement and the training session will be implemented in parallel with the ones in Target V.

Estimated cost:

- [EUR] costs of 2 WS
- [EUR] costs of TA for the requirements of Items (i) and (ii) – 15 expert - days

TASK 6 – Technical standards for cybersecurity in energy

The Group will cooperate and endeavour in achievement of the following targets:

6.1 Target VII – Application of ISO 27000 Series of standards

Develop and adopt a Methodology for the applicability, including a model for cost-benefit analysis, and Recommendations for application of the **ISO 27000** Series of technical standards in the context of cybersecurity in the energy sector – to be adopted / published in the format of applicable (optional) legal framework, and implemented at national level.

The activity will include the following steps:

(i) Define / agree on a set of criteria for assessment of cybersecurity risk alleviation impact of the ISO 27000 Series of standards, and identify a structure classifying the energy-relevant standards in different levels of scrutiny and/or applicability for different categories of stakeholders in the energy sector, including assessment of incurred cybersecurity risk and associated costs from non-implementation of the Standards, and SWOT analysis;

(ii) Develop draft Recommendations for application of the ISO 27000 Series of standards in cybersecurity for different categories of stakeholders in the energy sector (as defined in the description). The Recommendations shall include description of the effects, sensitivity analysis, criteria / methodology for cost-benefit analysis, reasoning and description of best practices on application of the standards in the EU and other domains;

(iii) Conduct consultation with the NRA via ECRB, CSIRTs and stakeholders - operators of critical infrastructures and providers of essential services, adjust the methodology;

(iv) Prepare the final consolidated version of the Recommendations along with an instrument for monitoring / reporting and support in application of the Standards, and propose to CyberCG for adoption and for publication in the Energy Community.

(v) Develop and agree on a mechanism for monitoring / reporting to CyberCG the developments in application of technical standards in cybersecurity by the Contracting Parties

The analytic and drafting work for the activities of Items (i) and (ii) shall be outsources and implemented through technical assistance (TA) of an expert team, which will provide the draft deliverables and corresponding information / training. The ToR for the TA shall be drafted by the ECS, and the comments / proposals related to these two Items shall be done by national representatives and NRAs as well as operators and providers of essential services as applicable, under responsibility of the focal points and ECRB and supported by ECS. Initial drafts for the Items (i), (ii), and (iv) shall be finalized by ECS. The CyberCG WG-CG representatives and ECRB shall support for the consultations of Item (iii) for each individual Party.

The methodology and the Recommendations shall be reviewed and approved by the ECRB.

Deliverables:

- ❖ Methodology on the applicability of ISO 27000 Series in the energy sector ;
- ❖ Recommendations / guidelines for application of ISO 27000 standards in energy;
- ❖ Workshop for the Methodology and draft Recommendations;
- ❖ Training session on the Methodology, Recommendations and application of the ISO 27000 Standards in energy – discussion, comparable reference with EU, effects on the energy market, options for enforcement, etc. – press release, publication.

Preconditions:

- Cooperation between cybersecurity authorities, energy stakeholders and NRA on national level;
- Technical assistance is needed for the Methodology and Recommendations;

Timing:

- Tentative duration of the overall activity is **15 months**. The consequent activities foresee continuous monitoring / reporting.

Estimated cost:

- [EUR] (costs of 2 WS)
- [EUR] (costs of TA for the requirements of Items (i) and (ii)) – 20 expert – days.

ANNEX 4

Energy Community Cybersecurity Networks
WORK PLAN 2020 - 2021

Cybersecurity Networks – organized and protected platform for exchange of information among a group of stakeholders, with restricted access – are established aiming to facilitate their direct cooperation and coordination, thus extending the use of cybersecurity-critical, sensitive information or services on regional level. Such communication and cooperation may include establishment and use of special communication channels and rules / protocols / technologies for data protection and access control.

Following Items 8 and 9 of the CyberCG Terms of Reference[28] and Point 10 of the Conclusions[29] from the First CyberCG Meting of 11 April 2019, the CyberCG has established Energy Community CSIRT Network. The **CSIRT Network** functions as a permanent panel for discussion on CSIRTs' operation in the energy sector – on the matter of operational cybersecurity relevance and on development and implementation of policies, measures and instruments to enable / support cybersecurity in the interconnected energy systems on the regional / Energy Community level.

The CSIRT Network operates through communication and exchange of information between national CSIRTs responsible for the energy sector, which may include energy stakeholders or experts – liaison officers or other categories of appointed officials from the operators of critical infrastructures and providers of essential services in the domain of the energy sector.

The CSIRT Network will achieve the targets with possibility of involving external participants (stakeholders, experts), where the exchanged data is not confidential or commercially sensitive. The CSIRTs are involved in development of coordinated or regional policies, as well as planning and training activities in cybersecurity in the domain of the energy sector, on Energy Community level.

By consolidating the CSIRT Network, CSIRTs may decide to establish an Energy CSIRT of the Energy Community (EnC CSIRT), available to all Parties and capable to provide support to national CSIRTs in protection of critical energy infrastructures or directly intervene, upon request of a national CSIRT or corresponding authority, in cybersecurity affairs in a specific country. In broader terms and according to mutual security protocols it may exercise its competences on bilateral, regional and broader level, in cases where competences or capacities of individual national CSIRTs are limited.

Complementary to the CSIRT Network, CyberCG may decide to support the establishment of one or more Energy ISAC(s) – Information Sharing and Analytical Centre(s), in the Energy Community. The E-ISAC (single – for energy, or separate – for gas / electricity / information technologies etc.) would facilitate direct communication and exchange of information on cybersecurity between stakeholders of a specific category / area in the energy sector. As its main feature, the E-ISAC includes stakeholders both from the public and private domain of the economy.

[28] https://www.energy-community.org/dam/jcr:a9163c92-fb05-40c3-a74c-acca91fe94c1/PA_02_2018_MC-EnC_CSCG_112018.pdf

[29] *https://www.energy-community.org/dam/jcr:6c7071f9-cc87-463d-9dcd-26604036936c/CyberCG_Conclusions_052019.pdf*

COMPOSITION

The CSIRT network consists of the representatives of participating Parties from the authorities responsible for cybersecurity, CSIRTs and the liaison officers responsible for cybersecurity in the companies that operate critical infrastructures and/or provide essential services, and ECS. The meetings may include participation of ENISA and invited experts. The CSIRT network may establish and apply instruments for confidentiality and its own internal structure of eligibility for access to different domains of its activities and/or corresponding information.

The official representatives (liaison officers) from the operators of critical infrastructures and providers of essential services shall complement the CSIRT participation in the Network in the context of all topics where information of relevance for the specific functions / services is exchanged or discussed. The CyberCG, supported by ECS, shall establish an instrument (statement, commitment) for confidentiality aimed to prevent disclosure of information considered classified, in cases such information has been exchanged or disclosed in the meetings.

DESCRIPTION

A general set of tasks for the CSIRT Network is outlined in Item 9.3 of the CyberCG Terms of Reference (based on Article 12 of the NIS Directive[30]). Subsequently, the Energy Community CSIRT Network is established to address cybersecurity on regional level in its performance:

a) as a permanent platform for discussion and exchange of information on CSIRT operations in the energy sector, such as resilience criteria, security of communication channels, threat analysis, early warning systems, applied standards, certification of the technologies, experience and best practices, and

b) as a working environment for communication and cooperation targeting the development of policies, structures, measures or instruments required for cybersecurity across the national borders – on regional and Energy Community level, in the environment of interconnected energy systems.

The information exchange categorized under a) is of operational character, addressing cybersecurity policies and practice in the energy sector on national level but also concerning coordination of bilaterally or regionally relevant criteria and measures. The CSIRTs shall have on disposal the facility of the Network to accomplish efficient exchange of operational information and best practices on relevant topics applied in the energy sector. Exchanges of information if this type are continuous.

The activities under b) relate to the development of the regional / Energy Community cybersecurity cooperation environment, with specific targets aiming at the establishment or enhancement of the means of communication and modes of cooperation. Items 9.3 f), g), j) and k) of the CyberCG Terms of Reference provide a basic scope of tasks. These type of activities are typically linked with specific targets and deadlines.

[30] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

In principle, the exchanged information should be of a non-commercially-sensitive character. The CyberCG shall endeavour to enhance the confidentiality mechanisms in the Network and security of the applied means of communication. Following Item 10 of the CyberCG Terms of Reference the CyberCG may decide to set up another layer of security and establish a Closed-CSIRT network aimed to expand the activities and communications in the domain of aspects considered as classified information on national level.

The CyberCG and the CSIRT Network may bring a decision to endeavour establishment of more condensed forms of cooperation, such as:

- Energy CSIRT of the Energy Community
- Energy ISAC(s) of the Energy Community

The Energy Community CSIRT shall have the authority to communicate directly with each national CSIRT's the information related to cross-border aspects of cybersecurity. It shall have the responsibility to directly engage in the assistance, and put on the disposal to any national CSIRT its capacity as required for applying cybersecurity policies and measures, preventing cyber attacks, building resilience and assisting in the protection of critical infrastructures. The CSIRT Network may engage in defining all aspects for the establishment of this CSIRT.

Establishment of an **Energy Community ISAC** (Information Sharing and Analysis Centre) complements the operation of the CSIRT Network. The ISAC may be established as a common centre for stakeholders from all domains of the energy sector, or as a sectoral (electricity, gas, oil, energy data protection / communication, energy producers, energy consumers, etc.). It is a permanent panel for the exchange of cybersecurity-critical or sensitive information between representatives of different companies connected to critical energy infrastructures or providing or receiving services in the same segment of the energy sector, from all Parties.

Energy Community ISAC is designed following the related public-private cooperation framework promoted by ENISA. As indicated in its Opinion Paper on ISAC Cooperation[31] of March 2019 the ISAC model offers several advantages such as:

- the model focuses on cooperation across borders and sectors;
- where there are multiple regulatory cybersecurity focused initiatives, it is a unique position to bring together the required public and private knowledge and expertise;
- the model allows for multi-layer cooperation from discussing strategic issues to operational challenges;
- the model requires no 'heavy' EU regulatory framework, but willingness for cooperation and sharing information based on trust, equality and transparency among Network and Information Security (NIS) experts;
- the model also increases cybersecurity information sharing at national level.

In order to avoid ambiguity among the stakeholders, ENISA recommends that the industry take the lead in creating sectoral ISACs, supported by ENISA. In the absence of industry not taking initiative, the public sector could fill the gap, (or vice versa).

[31] *file:///C:/Users/suz/Downloads/2019-03-15%20ISAC%20Opinion%20Paper.pdf*

The information Sharing and Analysis Centre (ISAC) operates as a central resource for gathering information on cyber threats (in many cases to critical infrastructures) and offers active sharing of information between the private and the public sector, between stakeholders with different levels and kinds of experience in cybersecurity – thus also performing as a training facility.

SCOPE OF ACTIVITY

TASK 7 –Energy Community CSIRT Network

The CSIRT Network operates through communication and exchange of information between CSIRTS, which may include specific category of stakeholders or experts, in the domain of the energy sector.

The CSIRT Network will cooperate and endeavour in achievement of the following targets:

7.1 Target I – Setup of Energy Community CSIRT communication platform

Establish and operate an electronic (online) communication platform dedicated to the Energy Community CSIRTS and representatives from data communication / system operation departments of the operators of critical infrastructure or the providers of essential services, authorised as CyberCG representatives in the CSIRT Network (WG CSIRT).

The communication channel provides discrete, restricted right of access to information and physical and semantic protection from access of unauthorised parties. The right of access is limited to the approved participants in the corresponding panel / topic for discussion, framed by a protocol and administered through agreed rules and procedures. The level of protection and applied technology is agreed among the participating CSIRTS and approved by the CyberCG.

Technical assistance shall be engaged for installation / implementation of the data protection technology, its operation and maintenance, and training of the participants.

The activity will include the following steps:

(i) Consider possible options for hosting the electronic platform for communication and financial / technical requirements for implementation of the dedicated communication platform, decide on the level and type of technical data protection and applied technology, and outline the options in Terms of Reference (ToR);

(ii) develop Rules for access and operation of the platform and for participation in the Panels, submit the proposal and draft Rules to CyberCG for adoption;

(iii) Following the technology guidelines and the ToR install the communication platform (HW / SW) and organize training for its use and for maintenance;

(iv) Upon establishment of the platform, set up the operational conditions, task and responsibilities and apply it in the communication, as indicated under a) and b);

The analytic work and the proposals shall be done by the representatives of the national CSIRTs and supported by ECS. Initial drafts for the Items (i) and (ii), and the logistic support for all Items shall be provided by ECS. The representatives shall provide expertise and contribute to the content for the ToR and the Rules, implement and obey the Rules. Extensive engagement and initiatives are requited from the representatives from the CSIRTs and assigned operators.

Deliverables:

- ❖ ToR for hosting, data protection criteria and applied technology for establishment of an electronic communication CSIRT platform;
- ❖ Rules for access and use of the CSIRT Platform;
- ❖ SW and HW modules (as applicable) for operation of the platform, rules for maintenance;
- ❖ Workshops / training sessions on the use of CSIRT communication Platform

Preconditions:

- Cooperation between cybersecurity authorities / CSIRTs and operators of critical infrastructure on the shared access to restricted data and common level of confidentiality;
- Availability of IT hosting environment and funds for the required communication technology

Timing:

- Duration of the installation activity is **5 months**.
- The consequent activities foresee continuous communication on the electronic platform and its maintenance.

Estimated cost:

- [EUR] costs of special technology (design, HW, SW) – incl. 10 expert - days
- [EUR] training workshop for the communication platform
- [EUR] costs of hosting and maintenance

7.2 Target II – CSIRT Panel for Cybersecurity Cooperation

Establish and operate a panel for discussion and exchange of information among CSIRTs, representatives from data communication centres of the operators of critical infrastructures and other invited stakeholders, as approved by the WG CSIRT, on cybersecurity operational issues relevant for the cybersecurity protection and the resilience and operational capacity of the critical infrastructures in the energy sector. The contents of communication can be:

a) incidental and service-oriented – referring to cybersecurity events, follow-up and new related developments, threats, incidents, and include related questions and comments, recommendations, advices etc. They can be bilateral or between a group in the panel (but in principle open to all members of the panel), and no formal follow-up is expected and no advanced or formal meeting scheduling is required. They can be near real-time, ex-post with respect to a significant event, or ex-ante with respect to estimated threats;

b) aggregated and topic-oriented – the topics are planned, selected form the list of proposals prepared in advance, and scheduled in an annual programme agreed by the Group. (The topics may include diverse aspects of cybersecurity, e.g. risk assessment methodologies, resilience criteria, certification of applied technologies, application of cybersecurity rules and standards, data access and confidentiality, level of preparedness of specific categories of stakeholders, etc. – as reflected in the energy sector). The discussions are online (exchange of files and teleconferencing), and on scheduled final meetings / workshops, followed by adoption of a document (conclusions, recommendation, rule, report, etc.) expressing the results of the discussion.

The online communication takes place on a dedicated electronic platform with restricted access. The exchanged information is treated as sensitive or confidential; the access is restricted and limited to the approved participants in the panel / topic.

The activity will include the following steps:

(i) Develop a Methodology for defining risk-response criteria and for impact analysis required for setting the format of activities under a), along with a corresponding Protocol for near-real-time exchanges of information focused on critical cybersecurity threats, events or incidents;

(ii) Identify the list of cybersecurity topics of interest as indicated under b), make the selection and develop draft Annual Programme (for 2020 and 2021) on the topics for discussion and targets (type of documents to be adopted, questions to be resolved) for each topic, along with timing for the meetings / workshops, and submit them to CyberCG for adoption.

(iii) Upon establishment of the platform, set up the operational conditions, task and responsibilities and apply it in the communication, as indicated under a) and b);

(iv) Organize the meetings (if required) and workshops for the selected topics (for broader audience, invited experts, etc.) – finalize and communicate the targeted acts.

The analytic work and the proposals shall be done by the representatives of the national CSIRTs and supported by ECS. Initial drafts for the Items (i) and (ii), and the logistic support for (i), (iii) and (iv) shall be provided by ECS. The representatives shall provide information for the Programme in item (ii) and conduct the activities under (iii) and (iv) for each individual topic in the Programme. Extensive engagement and initiatives are requited from the representatives from the cybersecurity authorities / CSIRTs in the communications under (iii).

Deliverables:

❖ Methodology and regional criteria for risk assessment and classification

❖ Rules and protocol for fast and real-time data exchange on the electronic communication CSIRT platform;

❖ Workshop on the protocol / mechanism for real-time assistance;

❖ Workshop / training sessions on cybersecurity emergency data exchange

Preconditions:

- Cooperation between cybersecurity authorities / CSIRTs and operators of critical infrastructure on the shared access to restricted data and common level of confidentiality;
- Availability of IT hosting environment and funds for the required communication technology

Timing:

- Duration of the installation activity is **14 months**.
- The consequent activities foresee continuous communication on the electronic platform and its maintenance.

Estimated cost:

- [EUR] costs of 2 WS

7.3 Target III – CSIRT Panel for Cybersecurity Planning and Education

Establish and operate a panel for discussion and exchange of information among CSIRT representatives and invited stakeholders on cybersecurity planning and education relevant for the energy sector. The contents of communication can be:

a) planning – exchanges on strategic developments and plans on cybersecurity in energy on regional level, including: adoption / implementation of (new) legislation, establishment of protected channels and means for restricted communication, rules and mechanism for cooperation with EU authorities or among national authorities on the regional issues, organization of regional cybersecurity exercises / stress tests, resolving disputes in the domain of cybersecurity between national authorities, etc.;

b) education – assessment of needs for professional training and general education on cybersecurity in the energy sector that can be executed in cooperation with the Energy Community Regulatory School. Activities may include exchanges on the available options and formats of training in cybersecurity, organization of training events for energy stakeholders on specific topics in cybersecurity, transfer of experience and best practices in cybersecurity from other areas in the energy sector, etc.

The online communication takes place on the same electronic platform as for 1.1, applied under b). All activities will have final meetings (as required) and follow-up conclusions or documents for adoption, workshops and training sessions shall be conducted according to available resources and experts.

The panel and related events may, as required by specific activities, include or engage representatives of authorities / CyberCG focal points, NRA, categories of stakeholders, academia and invited experts, as well as relevant EU institutions (EC, ACER, ENISA, ENTSO-E / ENTSOG, etc.).

The activities will include the following steps:

(i) Consider possible options for hosting the electronic platform for communication, decide on the level and type of technical data protection and develop Rules for operation of the platform and participation in the Panels, submit the proposal and draft Rules to CyberCG for adoption;

(ii) Identify the list of cybersecurity planning topics / areas of interest as indicated under a) and develop draft Annual Development Programmes (for 2020 and 2021) on the topics for discussion. Define the targets (type of documents to be adopted, questions to be resolved and other activities to be conducted) for each topic, along with timing for the meetings, and submit them to CyberCG for adoption.

(iii) Provide assessment on the needs for training / education on the one hand, and the available training options (TA) on the other hand, and create a corresponding Annual Training Programmes for training events (for 2020 and 2021) – both on the topics of interest for CSIRTs and for energy the stakeholders. Consolidate the Programmes with targets (type of training to be acquired or provided, questions to be resolved) for each training event, along with timing for the training sessions / workshops, and submit them to CyberCG for adoption.

(iv) Upon establishment of the platform, set up the operational conditions, task and responsibilities and apply it in the communication, as indicated under a) and b);

(v) Organize and conduct the meetings (if required), develop and submit to CyberCG for adoption the planning documents targeted in the discussed topics / areas outlined in the Development Programmes;

(vi) Organize and conduct the training sessions / workshops for the selected training events according to the Training Programmes.

The analytic work and the proposals shall be done by the representatives of the national CSIRTs and supported by ECS. Initial drafts of the Items (i), (ii) and (iii), and the logistic support for (i), (iv), (v) and (vi) shall be provided by ECS. The representatives shall provide information for the Programmes in item (ii) and (iii), and conduct the activities under (ii), (iii), (v) and (iv) for each individual topic / training event in the Programmes. Extensive engagement and initiative are requited from the representatives from the cybersecurity authorities / CSIRTs in the communications under (iv).

Deliverables:

- ❖ Rules for operation of an electronic platform and access to discussion panels;
- ❖ Annual Programmes (for 2020 and 2021) for discussion topics under Target I;
- ❖ Annual Development Programmes (for 2020 and 2021) for topics under Target II;
- ❖ Annual Training Programmes (for 2020 and 2021) for training / education under Target II that can be executed in cooperation with the Energy Community Regulatory School;
- ❖ Planning documents on the regional development of cybersecurity in the energy sector as defined in the Annual Development Programmes under Target II;
- ❖ Workshops / training sessions on cybersecurity for CSIRTs and for stakeholders (provided by CSIRTs) as defined in the Annual Training Programmes under Target II.

Preconditions:

- Cooperation between cybersecurity authorities / CSIRTs and energy authorities on regional level;
- Critical initiatives from national CSIRTs in using the Energy Community CSIRT Network in the proposed functions and formats.

Timing:

- duration of the overall activity is **24 months**. Initial setup and WS may last 4 months. The consequent activities foresee continuous communication on the electronic platform and through scheduled meetings / training events.

Estimated cost:

- [EUR] (costs of a WS)
  .
  Additional WS may be financed through other projects, or the donor community.

7.4 Target IV – Establishment of Energy Community Energy CSIRT

The Target shall be accomplished through CSIRT Network Planning activities, which would include the following steps:

(i) Nomination / identification of national energy CSIRT structures / units / teams responsible for energy systems digital information / operation channels security incident response;

(ii) Development and adoption of Rules for operation, annual work programme (for 2020) and certified communication means, and adopting a decision (by the CyberCG) on the establishment of a Closed[32] CSIRT Network for the Energy Community;

(iii) Operation of the Closed CSIRT Network within the CyberCG as a special function of the CSIRT network and building its capacity (if found necessary and applicable);

[32] *Following Item 10 of the CyberCG Termsof Reference*

(iv) Development and adoption of the rules for operation, criteria and sources of financing, tasks and responsibilities, constitutional documents for the establishment, internal codes of conduct and agreements for accreditation with the national authorities in the Energy Community and relevant international cybersecurity bodies, for the Energy CSIRT of the Energy Community – as the next step in consolidation of the Closed CSIRT Network into a self-standing CSIRT;

(v) Capacity building and education / training of the CSIRT.

The process includes eventual establishment of a Closed CSIRT Network within CyberCG (aimed to develop confidence, introduce procedures and apply best practice in the cooperation and mutual support) and its transition into an independent regional CSIRT responsible for the energy sector of the Energy Community (EnC E-CSIRT). Each of the steps / activities shall be further planned / elaborated in details by the CSIRT Network in the course of the planning period. The analytic work and the proposals shall be done by the representatives of the national CSIRTs and supported by ECS. Initial drafts of the required acts and the logistic support, and reporting on the results shall be provided by ECS.

Upon the establishment of the Energy Community CSIRT, the tasks / activities of the CSIRT Network shall be modified through a new work plan.

Deliverables:

❖ Rules and documents for the establishment and operation of the Closed SCIRT Network within CyberCG (optional);

❖ Rules and documents for the establishment and operation of the Energy Community Energy CSIRT;

❖ Program for training / capacity building of the Energy Community CSIRT.

(Additional items shall be defined in the course of planning by the CSIRT Network.)

Preconditions:

- Corresponding decisions to be taken by CyberCG, ECS, Energy Community Governance Bodies, national CSIRTs and national authorities;
- A sustainable form / source of financing to be identified and availability of funds to be confirmed;

Timing:

- Duration of the overall activity is **24 months (**the process of establishment is 12 months).. The implementation shall be delayed and establishment phase structured into planning and preparation phase, closed-CSIRT phase (if applied), accreditation period and preliminary training phase. The timing shall be elaborated in details in the course of planning, by the CyberCG CSIRT Network.

Estimated cost:

- [EUR] (costs of a WS)

TASK 8 – Energy Community Energy ISAC

The Energy ISAC (Information Sharing and Analysis Centre) operates through communication and first-hand exchange of information between the appointed representatives from participating energy stakeholders. Main areas of activity are the energy sector and related data protection and communication. Topics of interest cover applied cybersecurity policies, specific cybersecurity threats, incidents or applied protection measures, resilience criteria and measures, cyber protection plans and exercises and other types of best practice, as well as on planning, training and cybersecurity capacity building on company and customer level. On a reasoned proposal from the stakeholders, CyberCG may decide to establish separate ISACs for each relevant sector (e.g. electricity, gas, oil, communication).

The Tasks are applicable on each Energy Community ISAC in case more than one is established. The Targets and terms of implementation can be common or sector-specific.

The CyberCG shall endeavour in achievement of the following targets:

8.1 Target V – Establishment of Energy Community Energy ISAC

The Energy ISAC is a form of cooperation similar to the CSIRT Network. Its main feature is the link (communication, cooperation) between all companies, public and private, in the (specific) energy sector of the Energy Community, in the domain of cybersecurity.

The Target shall be accomplished through CyberCG activities, which would include the following steps:

(i) Develop and adopt the ISAC model, its functions and goals, rules for operation, tasks and responsibilities of the members and procedures for participation of stakeholders, and the involvement of national authorities in the Energy Community and relevant international cybersecurity bodies;

(ii) Communicate the draft proposal to national authorities and major stakeholders for comments and proposals for the topics of interest;

(iii) Consolidate and adopt the final documents along with a bi-annual Work Program with instruments for reporting, and the instrument (act) for enforcement, and submit the proposal to the CyberCG for adoption and further processing through the governance bodies of the Energy Community;

(iv) Establish a channel for electronic communication for the Energy Community Energy ISAC and adopt the rules for access and operation;

(v) Establish the initial operational setup of the ISAC and support the selection of convenor and adoption of the initial work program.

Some of the steps / activities shall be further planned / elaborated in details by the CSIRT Network in the course of the planning period. The analytic work and the proposals shall be done by the representatives of the national CSIRTs and supported by ECS. Initial drafts of the required acts and the logistic support, and reporting on the results shall be provided by ECS.

Deliverables:

- ❖ Rules and documents for the establishment and operation of the Energy Community Energy ISAC;
- ❖ Channel for electronic communication for the ISAC;
- ❖ Workshop and constitutional meeting of the ISAC.

(Additional items shall be defined in the course of planning by the CSIRT Network.)

Preconditions:

- Corresponding decisions to be taken by CyberCG, ECS, Energy Community Governance Bodies and national authorities;
- Interest of companies and national energy authorities for cooperation in the proposed format;

Timing:

- Duration of the overall activity on the establishment is **12 months**. The timing shall be elaborated in the course of planning by the CSIRT Network.
- ISAC should continue its operation according to adopted Work Plan.

Estimated cost:

- [EUR] (costs of a WS)
- Other costs may be defined in the course of planning.

8.2 Target VI – EnC ISAC Panel for support in certification

The E-ISAC of the Energy Community shall establish and operate a consultative Panel on certification and application of cybersecurity technologies and standards. For the members of the ISAC and, to the applicable level, the national energy regulatory authorities (NRA), the Panel shall include a coordinated system for exchange of information and best practice, expert-level consultations, education and cooperation with corresponding EU authorities including ENISA, on the following:

a) application of cybersecurity technical standards at corporate level
b) application of certified technologies in the energy sector
c) cybersecurity criteria and certification procedures of new technologies
d) cybersecurity standards / practices in the public domain and energy consumers protection

The Target shall be accomplished through the EnC ISAC Network, including cooperation / consultation with the Energy Community CyberCG WG on Governance and the ECRB, and include the following steps:

(i) Develop and adopt the ISAC draft Policy Paper / Guidelines for certification in the domain of cybersecurity in the energy sector covering at last the concepts for cooperation in a), b), c) and d), and submit it for further consultations and adoption by the CyberCG;
(ii) Communicate, via the CyberCG, the draft PP to the NRA, ECRB, ENISA and, as applicable to national certification bodies and EU certification authorities in the energy and information technology sectors;
(iii) Consolidate, adopt the final Guidelines on CyberCG level;
(iv) Establish a protocol for access and participation in the Panel, a schedule of topics and events, and proceed with consultation activities;

Some of the steps / activities shall be further planned / elaborated in details by the ISAC Network in the course of the planning period. The analytic work and the proposals shall be done by the ISAC participants and supported by ECS. Initial drafts of the required acts and the logistic support, and reporting on the results shall be provided by ECS.

Deliverables:

- ❖ Policy Paper / Guidelines on certification for cybersecurity in the energy sector;
- ❖ Panel on certification in cybersecurity – Rules / protocol for access and participation;
- ❖ Workshop / conference on cybersecurity certification in the energy sector.

Preconditions:

- Corresponding agreement and support by the EnC ISAC, ENISA and ECRB;
- Interest of companies and national energy authorities for participation / cooperation;

Timing:

- Duration of the overall activity on the establishment is **6 months**. The timing shall be elaborated in the course of planning by the ISAC Network.

Estimated cost:

- [EUR] (costs of a WS)