ENERGY COMMUNITY
CyberCG WORK PROGRAMME 2020 - 2021

VIENNA, 11 December 2019

Cybersecurity Coordination Group – 2nd Plenary Meeting

Energy Community

MC Procedural Act (29 November 2018) on the establishment of Energy Community Coordination Group for Cybersecurity and Critical Infrastructure (CyberCG)

- **Domains** (critical infrastructure / essential services)

  - Electricity / Natural gas / Oil / pollution and combustion emissions

  - Digital and electronic communications (services provided to energy operators)

- **Stakeholders**

  - Ministries (energy / climate / digital communications & information technologies), NRAs

  - Operators of critical infrastructures / essential services in energy (production / storage / TSO / DSO / PX / RSC)

  - National CSIRTs

Energy Community

MC Procedural Act (29 November 2018) on the establishment of Energy Community Coordination Group for Cybersecurity and Critical Infrastructure (CyberCG)

- ### Tasks

  - establish administrative and operational environment (focal points / liaison officers)

  - communicate information (reports / strategies / measures) and knowledge (training / research and development / public awareness)

  - Develop and apply EU-coherent methodologies for risk assessment (security criteria) and identification and designation of essential services / critical infrastructures

  - apply the relevant EU technical standards on information security and relevant technologies

  - establish a CSIRTs network (security incidents and threats / capacity building / cooperation and early warning / mutual assistance)

  - facilitate cooperation with EU MSs / gaining closer relations with ENISA

Plenary Meetings

- take place **twice a year** (May - June, November - December)

Forms of activity

- WG on Energy Community **Critical Infrastructures** and Essential Services **(WG-ECCI)**
- WG on Energy Community **Cybersecurity Governance (WG-ECCG)**
- establishment and operation of Energy Community **Cybersecurity Networks (CSIRT, ISAC)**
- organization and operation of Energy Community **Cybersecurity Academy**
- the role of the **Focal Points** and **stakeholders**
- the role of the Energy Community **SECRETARIAT** and **ECRB**
- cooperation with EU institutions **(EC, ENISA, ENTSO-E, ENTSOG, EE-ISAC, CSIRTs…)**
- common events and forms of cooperation with the **donor community** and **academia**
- activities in the **public domain**

- **COMPOSITION**

  - ministries, NRA, liaison officers / representatives from operators of ECI and EES

- **Mandate** at national and regional (Energy Community / cross-border) level in the domain of energy

  - support / facilitate / develop coordinated criteria and mechanisms for identification and nomination of ECI and EES

  - support / facilitate development of measures for increased security and resilience of ECI and EES (Operator Security Plans) and establishment of mutual defence mechanisms

  - define common / coordinated criteria for Risk Assessment and identification / categorization of cyber threats / attacks

  - define mutual test scenarios and organize coordinated trial exercises

  - establish a system of reports and recommendations

Tasks	Targets / Activities	2020				2021			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

WG on ENERGY COMMUNITY CRITICAL INFRASTRUCTURES (WG-ECCI)

Tasks	Targets / Activities
IDENTIFICATION AND DESIGNATION OF CRITICAL ENERGY INFRASTRUCTURES AND ESSENTIAL SERVICES	**1.1 Report on the status of Energy Critical Infrastructures (ECI) and Essential Services (EES)**
	- ECI / EES reporting templates, mechanism [ECS, WG]
	- completion, approval, publication [ECS, WG] - Workshop on the Energy Critical Infrastructures
	- monitoring and reporting on ECI / EES status
	1.2 Common platform for regional designation of ECCI
	- draft Rules for identification / designation of ECCI [ECS]
	- completion, adoption of ECCI Rules and AP [ECS, WG] - workshop on ECCI cross-border Designation Rules and Action Plan
	- enforcement of ECCI rules between the Parties [WG]
	- monitoring and assistance [ECS]

Tasks	Targets / Activities	2020				2021			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
WG on ENERGY COMMUNITY CRITICAL INFRASTRUCTURES (WG-ECCI)									
ENERGY OPERATORS' SECURITY PLANS (OSP)	**2.1 Guidelines for Operator Security Plans (OSP)**								
	- status Report on security plans / liaison officers								
	- TA on Operator Security Plans (drafting) - Methodology and Guidelines								
	- Guidelines on OSP – development / adoption [ECS, WG] - workshop on Operator Security Plans & Methodology								
	2.2 Regional Implementation of Operator Security Plans (OSP)								
	- TA on Methodology for regional Risk Analysis								
	- Rules for regional cyber threat exercises [ECS, WG] - workshop on regional Risk Analysis								
	- monitoring and assistance [ECS]								
	- development / adoption of Guidelines on regional Risk Analysis [ECS]								
	- workshop on the regional cyber threats / OSP exercise								
	- regional mechanism for cooperation and ECCI resilience support [WG, Parties]								
	- workshop on regional cybersecurity (resilience) planning								

- **COMPOSITION**

  - ministries (energy / cybersecurity / infrastructure), NRA, responsible standardization authority

- **Mandate** at national and regional (Energy Community) level, in the format relevant for the energy sector

  - support coordinated criteria / process for transposition and implementation of EU cybersecurity-related legislation and recommendations (in particular ECI Directive, NIS Directive, other related acquis)

  - support / facilitate coordinated cybersecurity planning mechanisms – cybersecurity strategies, coordinated efforts for establishment / implementation of common Energy Community Strategy for Cybersecurity

  - develop a common platform for regulatory criteria related to cybersecurity in the energy sector regulation (certification / tendering, price regulation) – in coordination with ECRB

  - develop common / coordinated criteria for application of technical standards related to cybersecurity (ISO 27000 Series, other standards) – in coordination with ECRB

Energy Community

Tasks	Targets / Activities	2020				2021			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
WG on CYBERSECURITY GOVERNANCE IN THE ENERGY COMMUNITY (WG-CG)									
ACQUIS ON CYBERSECURITY	**3.1 Adaptation of the ECI Directive for the Energy Community**								
	- ECI Directive – adjustments [ECS] - Report on the current state of compliance								
	- ECI Directive – coordination on early implementation, Action Plan [CyberCG] - workshop on legal transposition of ECI Directive								
	- monitoring and assistance [ECS]								
	3.2 Adaptation of the NIS Directive for the Energy Community								
	- NIS Directive – adjustments [ECS] - Report on the current state of compliance								
	- NIS Directive – coordination on early implementation, Action Plan [CyberCG] - workshop on legal transposition of NIS Directive								
	- monitoring and assistance [ECS]								
	3.3 Guidelines on implementation of cybersecurity acquis								
	- Guidelines on implementation of Cybersecurity *acquis* in the Energy Community - workshop on application of Cybersecurity Law in energy								

Tasks	Targets / Activities	2020				2021			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

WG on CYBERSECURITY GOVERNANCE IN THE ENERGY COMMUNITY (WG-CG)

Tasks	Targets / Activities
CYBERSECURITY STRATEGIES FOR ENERGY SECTOR	**4.1 Report on the current Cybersecurity Strategies in energy** - criteria for gap analysis in cybersecurity strategies [ECS] - Report / gap analysis on existing cybersecurity strategies - technical workshop on Cybersecurity Strategies in the Energy Community - monitoring and assistance [ECS] **4.2 Cybersecurity Strategy of the Energy Community** - common methodology / criteria for coordinated cybersecurity planning [ECS] - technical workshop on cybersecurity planning methodology - draft regional cybersecurity strategy for the Energy Community [ECS] - training workshop on regional cybersecurity planning

Energy Community

Tasks	Targets / Activities	2020				2021			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
WG on CYBERSECURITY GOVERNANCE IN THE ENERGY COMMUNITY (WG-CG)									
REGULATORY TREATMENT OF CYBERSECURITY IN ENERGY	**5.1 Cybersecurity in certification and tendering of new infrastructure**								
	- TA on methodology and guidelines for minimum compulsory cybersecurity criteria								
	- workshop on cybersecurity criteria in tendering								
	- Guidelines on cybersecurity criteria in certification and tendering of new ECCI [ECRB]								
	5.2 Cybersecurity in regulated prices and tariffs								
	- TA on methodology and criteria for calculation of cybersecurity costs in energy regulation								
	- workshop on cybersecurity costs in tariffs								
	- Guidelines on cybersecurity criteria and rules for calculation of cybersecurity costs [ECRB]								
	- training workshop on the regulatory treatment of cybersecurity costs								
	- monitoring and assistance on regulatory treatment of cybersecurity [ECS, ECRB]								

Energy Community

Tasks	Targets / Activities	2020				2021			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

WG on CYBERSECURITY GOVERNANCE IN THE ENERGY COMMUNITY (WG-CG)

Tasks	Targets / Activities
TECHNICAL STANDARDS FOR CYBERSECURITY IN ENERGY	**5.3 Application of ISO 27000 and other Standards in cybersecurity in the Energy Community**
	- Report on the use of ISO 27K and other standards in cybersecurity in energy [ECS, ECRB] - workshop on the status of application of ISO 27K and other cybersecurity standards in energy
	- TA on methodology and Guidelines for ISO 27K and other cybersecurity Standards application in energy
	- workshop on ISO 27K methodology and Guidelines
	- Guidelines for application of ISO 27K and other standards drafting / adoption [ECS, ECRB]
	- training workshop on the Guidelines for ISO 27K and other Standards application in Energy
	- monitoring and assistance on ISO 27K application [ECS, ECRB]

Energy Community

- **COMPOSITION**

  - ministry (cybersecurity), CSIRT, liaison officers / representatives from operators of ECI and EES

- **Mandate** at Energy Community / EU cross-border level, among the CSIRTs / ISACs and related authorities / operators

  - establish a secure, dedicated communication platform available to CSIRTs and associated, registered officials

  - establish a communication network and protocols for exchange of applicable, operational information on cyber threats / attacks, forensics and related measures, as well as for near real-time support

  - establish a communication network for exchange of strategic, planning information on cyber resilience, recovery aspects, redundancy / availability of support capacity, as well as on education / training in cybersecurity

  - establish an Energy Community Energy CSIRT structure for cooperation and sharing national cybersecurity resources

  - establish an Energy Community Energy ISAC as a platform for communication / cooperation / education in cybersecurity between energy stakeholders / partners / service providers – in the format of public-private partnership

CyberCG Work Programme 2020 – 2021 Cybersecurity Networks

Tasks	Targets / Activities	2020				2021			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
ENERGY COMMUNITY CYBERSECURITY NETWORKS									
ENERGY COMMUNITY CSIRT NETWORK	**6.1 EnC - CSIRTs electronic platform (setup)**								
	- review of existing communication channels / initiatives - review of options for hosting a communication platform								
	- conceptual design, technical requirements / setup, rules of procedure for secure operation [ECS]								
	- TA - SW installation and trial operation								
	- workshop on the EnC CSIRT communication platform [CSIRT WG]								
	- operation of the communication platform (Parties)								
	6.2 CSIRT Panel for Cybersecurity Operations (setup)								
	- methodology for regional risk criteria and assessment								
	- rules / protocol for real-time exchange of information								
	- workshop on the mechanism for real-time assistance								
	- CSIRT panel protocol TRIAL								
	- training exercise on emergency data exchange								
	- monitoring and assistance								

Energy Community

Tasks	Targets / Activities	2020				2021			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4

ENERGY COMMUNITY CYBERSECURITY NETWORKS

ENERGY COMMUNITY CSIRT NETWORK	**6.3 CSIRT Panel for Planning and Education (setup)**								
	- rules / protocol for cooperation in CSIRT planning [ECS]								
	- training needs in energy forensics [CSIRT]								
	- program for education and training / action plan [ECS]								
	- workshop on CSIRT planning / education [CSIRT]								
	- assistance and support								
	6.4 Establishment of Energy Community CSIRT								
	- review on existing national CSIRT structure / capacity								
	- establishment of national ENERGY CSIRT structures								
	- criteria on the establishment of Regional Energy CSIRT(s) in the Energy Community (E-CSIRT)								
	- rules / protocol / Programme of activities for a regional energy CSIRT								
	- workshop on the operation of a regional E-CSIRT								
	- assistance and support								

Energy Community

Tasks	Targets / Activities	2020				2021			
		Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
ENERGY COMMUNITY CYBERSECURITY NETWORKS									
ENERGY COMMUNITY ENERGY ISAC (EnC-ISAC)	**7.1 Establishment of Energy Community Energy ISAC**								
	- conceptual design of the EnC ISAC operation platform								
	- conference on PPP and cooperation between energy stakeholders in cybersecurity								
	- rules / protocol for cooperation of energy enterprises [CyberCG]								
	- program for operation and forensic education / training and Action Plan [CyberCG]								
	- TA – SW on electronic platform for the EnC-ISAC								
	- kick-off workshop on establishment of EnC-ISAC								
	- assistance and support [ECS]								
	7.2 EnC-ISAC Platform for support in certification								
	- Guidelines on certification criteria / policy for the Energy Community stakeholders								
	- Rules / protocol for support in certification in the energy sector								
	- conference on cybersecurity certification in the Energy Community								
	- assistance and support [ECS]								

FORMAT

- Energy Community (CyberCG / ECRB) brand for its education and training activities in Cybersecurity

- including workshops (related to Work Plans 2020-2021 for WG / TA / CS networks), training events and seminars, closed events in CSIRTs / ISACs networks, conferences, as well as public events

- at Energy Community / EU / international level – all categories of stakeholders

- ECS – established, or in coordination / joint organization

Content (and related cybersecurity context)

- legislative / regulatory framework, cybersecurity technical standards, communication protocols / technology

- CyberCG - developed / adopted acts, rules, methodologies, protocols, guidelines, recommendations, plans, strategies,

- risk scenarios / exercises, criteria and conditions, cyber threats, support mechanisms, cybersecurity assistance

- energy technologies, energy / data communication systems, energy infrastructure

- communication protocols / technology, confidentiality, data protection, cyber threat information, cyber forensics

Energy Community

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

THANK YOU
FOR YOUR ATTENTION and COOPERATION

simon.uzunov@energy.community.org

🌐 www.energy-community.org

🐦 Ener_Community

in /company/energy-community

f /Ener.Community

▶ /EnergyCommunityTV