Draft 01v2 – 10 June 2020

Establishment of
ENERGY COMMUNITY ENERGY ISAC

WHITE PAPER

Vienna, June 2020

INTRODUCTION

The Energy Community cybersecurity dimension was established by the Ministerial Council in 2018[1], and already promoted its mission through the Cybersecurity Coordination Group[2] (CyberCG) activities and the Cybersecurity Study[3] completed in 2019. In 2020, we are heading to another initiative to set a new layer of cooperation in the cybersecurity landscape of the Energy Community by the establishment of an energy **Information Sharing and Analysis Centre** (EnC ISAC).

The ISAC security cooperation model is used in many countries or sectors and considered as highly efficient. It was first applied in the USA in 1997 as a measure to support cooperation between public and private sector in the protection of critical infrastructures. To date, it is applied in 25 areas of the economy and the social domain. US ISACs collaborate through the National Council[4] established in 2003. National sector-specific ISACs also exist in Japan, India, Canada and other countries. Large ISACs of global relevance are the Aviation ISAC, AUTO-ISAC, Health-ISAC, Financial Services (FS-ISAC), etc.

In the EU, national sector-specific ISACs exist in many counties such as Poland, Norway, Finland, Belgium, Netherlands and others. Some EU countries (Spain, Portugal, Lithuania, Luxemburg,) have established ISACs to aggregate national resources from different sectors. EU-wide, sector-specific ISACs are set in the financial institutes, railways and energy sector. European ISACs enjoy the support of the European Cyber Security Organization[5] (ECSO) and the EU Agency for Cybersecurity[6] (ENISA).

There is no ISAC structure covering the Energy Community Contracting Parties so far. On the other side, the Cybersecurity Study indicated shortcomings that may require such a treatment – among others (*Executive Summary*, p.4):

- Energy security issues are often addressed only at the country level, without considering the complexity of interdependence of the EnC CPs and EU Member States;
- There is a need to create public-private partnerships when sharing information. Under existing legislation, cybersecurity requirements differ between public and private stakeholders.

ISACs

ISACs are member-driven organizations delivering all-hazards threat and mitigation information to asset owners and operators.

Information Sharing and Analysis Centers help critical infrastructure owners and operators protect their facilities, personnel and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency. ISACs reach deep into their sectors, communicating critical information far and wide and maintaining sector-wide situational awareness.

© 2020 National Council of ISACs
https://www.nationalisacs.org/

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

[2] https://www.energy-community.org/events/2019/12/CYBERCG.html

[3] https://www.energy-community.org/dam/jcr:db8e479d-b423-40c9-9ff9-998c7d9045ef/Blueprint_cyber_122019.pdf

[4] https://www.nationalisacs.org/

[5] https://ecs-org.eu/

[6] https://www.enisa.europa.eu/

Furthermore, the Study Report explicitly recommends establishing an energy ISAC – as a public-private partnership that will support the energy companies by enabling trust-based data and information sharing (Title 7.1.1 *Recommendations for the EnC level framework*, p.162).

This proposal is based on the model of the EU Energy ISAC[7] (EE-ISAC) and criteria compatible with the ECSO *Position Paper on European Sector-Specific ISACs*[8] (December 2018) and the ENISA study report *ISACs Cooperative models*[9] (February 2018).

WHY JOINING THE ENC ISAC CAN BENEFIT YOUR ORGANIZATION?

In the EnC ISAC you can have:

- Active personal contacts with other companies and bodies, who face similar challenges in cybersecurity as you
- Access to sensitive information on cybersecurity threats, and solutions and best practices to tackle them
- Assistance from other Members to your cybersecurity policies and problems
- Opportunity to participate and contribute to the development of standardization and certification procedures
- A role in development and implementation of cybersecurity-related legislation
- A public-private partnership platform and security cooperation with non-industry experts

PROPOSED ENERGY ISAC MODEL

Objectives

Primary objective of the EnC ISAC is to enable efficient and safe sharing of critical information, experiences and best practices between diverse energy stakeholders in order to increase the level of their cybersecurity. It will provide data for analysis and common access to the findings.

The ISAC will also facilitate the building of resilient infrastructures, standardization and certification procedures, implementation of ECI and NIS Directives, as well as training, capacity building and overall transparency in the field of cybersecurity.

ISACs

The ISACs are non-profit organizations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) as well as allow two-way sharing of information between the private and public sector.

ISACs have created communities within the private sector. They could be oriented on a specific critical sector (e.g. finance, energy, health) or serve as a focal point on the national level to gather information about cyber incidents and analyse it.

They create an ecosystem in which trust is being built among critical operators and experience can be shared. Because of this, entities less advanced in the field of cybersecurity could learn from others.

To ensure the right level of cybersecurity, cooperation between the public and the private sector is absolutely crucial.

© ENISA – *ISAC Cooperative models* STYUDY REPORT
https://www.enisa.europa.eu/

[7] https://www.ee-isac.eu/

[8] https://ecs-org.eu/documents/publications/5c0a6a3aac673.pdf

[9] https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

Members

The ISAC expands the domain of cooperation across the borders and it brings together different categories of stakeholders that can bring added valued in the energy sector cybersecurity.

- The EnC ISAC will be established by, and for the benefit of, both state-owned (public) and private operators of infrastructures and energy utilities. They should be strongly represented in the membership in order to bring energy sector priorities in the focus. Operators of critical infrastructure and providers of essential services are the first to fall in this category.
- Companies involved in the energy supply chain – technology providers and producers of equipment, facilities and construction parts, including those related to storage, climate and environmental services and may contribute to the added value.
- Cybersecurity service and technology providers that can contribute in achieving the ISAC's targets. Participation in the ISAC may turn their attention to energy-specific solutions and services.
- Cybersecurity authorities, regulators and CSIRTs or their associations that can share their experience, but also benefit from the ISAC activities in creating the national cybersecurity environment and the application of standards.
- Institutes and universities involved in cybersecurity research and teaching that can provide valuable expertise and analysis of the critical information, and capacity for education and training.
- It is suggested to differentiate between Members and Partners. Members bear full responsibility for the ISAC operation and sharing information, but also enjoying full access to the analysis and resulting benefits. The membership in the ISAC is voluntary, based on the potential for added value, and mutual trust. Members must follow the agreed confidentiality rules. Partners cooperate with the ISAC through custom arrangements (memoranda) with specific targets and cooperation area, no steering powers, limited access to information and no confidentiality obligation.

The operation of the ISAC is based on trust and confidence between the stakeholders. The members are expected to commit to, and withstand non-disclosure of the sensitive information shared within the ISAC. Potential stakeholders with an obligation for reporting to non-member authorities cannot acquire membership status.

The ISAC shall operate through meetings – closed or open to non-members, and Working Groups set-up around specific technologies, problems or targets. It shall be steered by a Plenary Assembly, and supported by a Board and assisted by the Energy Community Secretariat.

ISACs

We need ISACs that can provide information in the right model with an added value that can put the intelligence between the ISAC and the final user. ISACs are also important in the context of the implementation of the NIS Directive as they can facilitate the sharing of best practices, harmonisation of specific requirements, and collaboration between Operators of Essential Services.

A new and agile structure should be established for sector-based ISACs in Europe, one which fits with the requirements of each sector and which is able to collaborate with national ISACs and other relevant stakeholder communities, in a trusted and operationally driven environment.

An energy ISAC should avoid duplicating efforts in activities or sharing of information already ensured by other organizations.

© ECSO – *European Sector-specific ISACs* POSITION PAPER, December 2018
https://ecs-org.eu/

Main activity in the ISAC is sharing cybersecurity-relevant information between the members. The ISAC may also coordinate and support its members in the process of certification, application of technical standards, development of regional rules and protocols, and in capacity building activities.

INFORMATION SHARING

As trust is the basic principle, so is non-disclosure of the shared sensitive information. For that purpose, the ISAC will adopt and members will apply and obey, a classification pattern consisting of four levels of restriction from access (WHITE, GREEN, AMBER and RED) applied to each item of sensitive information.

Furthermore, the ISAC will apply and enforce a correlated commitment for non-disclosure (confidentiality) of the shared information by each member, along with the rules and means for publication.

Information shall be shared in physical or virtual meetings (through internet channels with specified technology and level of protection). The information to be shared and analysed may include:

- Cybersecurity events and incident management
- Cybersecurity threats – observation and evaluation
- Exercises, threat modelling, simulation events and analysis
- Applied security plans and practices
- Applied regulations and technical standards on cybersecurity
- Applied cybersecurity technologies and services
- Analysis of cybersecurity environment and public domain
- Education and training events

The participation of research institutes and academia will provide added value in the analysis of the security-related information and in capacity building.

LEGAL FORMAT

The Energy Community ISAC will be established by its Founding Members as a non-profit association under Austrian law, formally seated in Vienna. The Secretariat may provide support in drafting the Articles of Association.

The rights and obligations of each member will be defined in Articles of Association. Accession of new members would be based on the possible added value and articulated in a way to preserve the level of confidence in the trusted environment. These and other administrative aspects of its operation will be outlined in the Terms of Reference.

The financing of the ISAC operation would be done through a mandatory membership fee, defined and agreed in the Articles of Association. The expenses to be covered will include:

- Costs of establishment and maintenance of protected communication channel
- Costs of engaged (outsourced) services
- Costs of (internal) education and training exercises
- Honorarium for the Chairperson and the (five) Board members

- Costs for hosting of physical events (meeting room and catering) in case the Secretariat is not involved

Costs of travelling and accommodation for the representatives during physical meetings and other specific expenses are normally borne by the members.

In the initial period (before permanent ISAC infrastructure and procedures are established), the Energy Community Secretariat may host the meetings and communication requirements. The Secretariat will provide administrative support to the ISAC within the limit of its resources. It will participate in the ISAC operation and support the ISAC activities without a decisive (voting) right, and facilitate its coordination with the rest of the energy environment, such as ministries and regulators.

Energy Community ISAC

The first steps of the interested company / authority toward the establishment of the EnC ISAC is confirmation to the Energy Community Secretariat of its interest and commitment for participation in the set of no less than five Founding Members.

Vienna, 10 June 2020