Terms of Reference for the ENISA Industry 4.0 Cyber Security (EICS) Experts Group

ENISA launches this Call for Participation to invite experts in security of Industrial implementations of *Internet of Things* to participate in its expert group.

The ENISA Industry 4.0 Cyber Security Experts Group (EICS) is an evolution of the ENISA ICS Security Stakeholder Group (call 2014- 2017) which aims at gathering experts at the crossroads of industrial systems and *Internet of Things* to exchange viewpoints and ideas on cyber security threats, challenges and solutions.

1 Background

ENISA defines *Internet of Things* as an emerging concept describing a wide ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context. Internet of Things is tightly bound to cyber-physical systems and in this respect is an enabler of Smart Infrastructures by enhancing their quality of service provisioning.

The threats and risks related to Internet of Things devices and services are manifold and they evolve rapidly. With great impact on citizens' safety, health and privacy, the threat landscape concerning Internet of Things is extremely wide. Hence it is important to understand what needs to be secured and to develop specific security measures to protect Internet of Things from cyber threats.

ENISA Industry 4.0 Cyber Security Experts Group is an information exchange platform that brings together experts to ensure security and resilience of the entire Internet of Things ecosystem in industrial implementations.

Experts of the EICS group shall have technical background expertise and direct exposure on one or several of the following:

- Internet of Things with a focus on smart industry, Industry 4.0, Industrial IoT, Smart manufacturing, Smart logistics, robotics and AI applied to industrial environments and Operators of essential services;
- Suppliers and developers of Internet of Things hardware and/or software for industrial environments;
- Associations and not-for-profit organisations involved in Internet of Things security on top of legacy infrastructure and industrial environment;
- Regulation bodies, academia, standardisation bodies and policy makers directly involved in the above topics.

2 Objectives

With the objective of making Internet of Things more secure, ENISA develops information exchange among communities, organises annual studies and workshops, and continuously engages the operational community through the experts group.

Participants to the EICS group shall contribute to enhance the current level of cyber security of the Internet of Things in industrial implementations by sharing their expertise on current threats, challenges and solutions.

The scope of the EICS group is focused on securing the entire ecosystem of Internet of Things in industrial implementations as well as the communications and interactions with the physical world that may impact safety.

Your role in the experts group would be:

- To contribute to relevant position and policy papers on security topics in the domain of the Internet of Things in industrial implementations;
- To exchange knowledge with other participants and ensure the convergence of current and future cyber security efforts;
- Discuss other on the approaches taken towards protecting Internet of Things systems in industrial implementations (policy, good practices, standardisation…)

Members of the EICS group have the following benefits:

- Orient and review ENISA studies by sharing their experience on current threats and good practices;
- Possibility to attend ENISA workshops or other related events regarding to the security of Internet of Things in industrial implementations;
- Exchange information with other experts from the sector in a trusted manner;
- Direct contribution to ENISA's work with the possibility to express their opinion on current and future policy.

3 EICS group Group Members

Member of the Experts Group can be:

1. Individuals appointed in their personal capacity.
2. Individuals appointed to represent a common interest shared by stakeholders in a particular policy area; they shall not represent an individual stakeholder.
3. Organisations in the broad sense including companies, associations, governmental and non-governmental organisations, universities, research institutes, European Union Agencies and Bodies, international organisations.

Involved individuals are selected based on excellence in the following skills (indicatively):

- Knowledge of technical, policy and regulatory issues at national and/or pan European level regarding smart industry, Industry 4.0, Industrial IoT, Smart manufacturing, smart logistics, robotics and AI applied to industrial environments and OES;
- Direct experience on smart industry, Industry 4.0, Industrial IoT, Smart manufacturing, smart logistics, robotics and AI applied to industrial environments and critical infrastructures from a security perspective. A focus on cyber security for safety would be considered a plus;
- Technical background on cyber security on smart industry, Industry 4.0, Industrial IoT, Smart manufacturing, smart logistics, robotics and AI applied to industrial environments and critical infrastructures;
- Experience and/or good understanding of cyber security;
- Experience from interaction with relevant stakeholders/users;
- Active participation in other relevant communities.

The working language is English.

In addition to the above mentioned skills, the review of applications will also take into account the following criteria:

- Individuals are appointed to represent a common interest shared by the type of stakeholders; as such they do not represent an individual stakeholder;
- The formation of the group will be done in a way that a mix of skills in the area of security and resilience of the Internet of Things, sector and geographic coverage is taken into account;
- Limited number of experts in order to efficiently interact in achieving desired outcomes; (maximum 15 members and 5 alternate members);
- Interest or motivation of the Expert in regard to the technical area;
- General background of the Expert in the technical area;
- Gender balance.

4 Administrative information

4.1 Approach/ Working Methods

The structure of the reference group is organized around periodic conferences calls, mailing list and a space on the resilience portal website. Members will be asked to provide input on ENISA work in the area and highlight trends and current operational issues. In addition to the contribution of the Experts Group to the collection of requirements and ideas, the group will contribute to the review of ENISA deliverables of related projects. Experts will be acknowledged in potential related ENISA reports as contributors.

The main means of interaction of the ENISA Industry 4.0 Cyber Security Experts Group will be online tools (web conferencing, mails, and phone) and the dedicated portal. One physical meeting could be held once a year. The arrangements of this meeting are going to be discussed and agreed with the group members.

4.2 Organisational modalities

A long term commitment by the group members is desirable. The contribution of each member of the ENISA Industry 4.0 Cyber Security Experts Group is roughly estimated with circa 2 person days per year. This engagement does not include the time required for a potential physical meeting.

The effort of members invested in the ENISA Industry 4.0 Cyber Security Experts Group activities will not be reimbursed by ENISA.

The travelling expenses of ENISA Industry 4.0 Cyber Security Experts Group related to a potential physical meeting will not be reimbursed. ENISA is going to facilitate the organisation of a possible meeting by means of the meeting venue and catering.

From each conference call and meeting, short result oriented minutes will be drafted and sent for approval to the ENISA Industry 4.0 Cyber Security Experts Group members.

4.3 Data protection

Personal data of participants in Informal Expert Groups will be processed in accordance with Regulation 2018/1725[1] on the protection of individuals with regard to the processing of personal data by the Union

[1] https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=uriserv:OJ.L_.2018.295.01.0039.01.ENG&toc=OJ:L:2018:295:TOC

institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

4.4 Transparency

The members and Chair of the reference group are subject to the requirement of confidentiality pursuant to article 287 of the Treaty for the Functioning of the European Union, even after their duties have ceased. In particular without prejudice to the provisions of Regulation (EC) No. 45/2001, they shall be required not to disclose information of the kind covered by the obligation of professional secrecy, such as information about undertakings, their business relations or their cost components, as well as information relating to the investigation of criminal offences and the application of criminal law.

4.5 Duration of this Call

This Call for Expression of Interest inviting experts to the ENISA Industry 4.0 Cyber Security Experts Group remains open for a period of 1-3 years during which applications are invited and periodically evaluated. Eligible candidates will be entered on a roster from which they will be selected to join either as members or as alternate members. If during the course of the Group, there are vacancies in the membership of the Group, they will be firstly filled by willing alternates and secondly by eligible candidates from the roster.