TERMS OF REFERENCE FOR THE ENISA EHEALTH SECURITY EXPERTS GROUP

1. BACKGROUND

The ENISA eHealth Security Experts Group is the second iteration of the expert group focusing in the healthcare sector, initially created in 2015. The creation of this Experts Group aims at gathering experts from the Healthcare sector to exchange viewpoints and ideas on cyber security threats, challenges and solutions and to support ENISA in its work in the sector, in view of the Agency's new mandate.

Studies have shown that cyber security incidents in eHealth systems can have a great societal impact. This fact is reflected in the specific inclusion of the Healthcare sector as one of the sectors of Essential Services in the NIS Directive. As Healthcare becomes more connected and reliant on networks and information systems, protecting these systems from cybersecurity incidents becomes critical, especially when considering their potential impact on the availability of these services and even on patient safety.

ENISA started working on the eHealth security topic in 2015 and has published a number of deliverables, while supporting associated regulatory developments in the EU. With the objective of making eHealth more secure, ENISA develops information exchange among communities, organises annual studies and workshops, and continuously engages the operational community through the experts group.

The ENISA eHealth Security Experts Group is envisaged as an information exchange platform that brings together experts to ensure security and resilience of the Healthcare sector in Europe. The eHealth Security Experts Group brings together technical experts on healthcare information systems, cyber security and contingency, with representatives from service providers, healthcare organisations, healthcare authorities, academia and standardisation bodies.

Experts of the ENISA eHealth Security Experts Group shall have technical background expertise and direct exposure on one or more of the following:

- Operators of eHealth systems and services (healthcare organisations, national eHealth service providers etc.) with responsibilities for cyber security in their organisations;
- National competent authorities for eHealth/Healthcare services;
- Manufacturers or integrators of medical devices or healthcare information systems with a focus on cyber security;
- Associations and not-for-profit organisations involved in eHealth security;
- Relevant authorities, academia, standardisation bodies and policy makers directly involved in the above topics.

2. OBJECTIVES

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

Participants to the ENISA eHealth Security Experts Group shall contribute to enhance the current level of cyber security of Healthcare by sharing their expertise on current threats, challenges and solutions.

The scope of the ENISA eHealth Security Experts Group is focused on securing the entire ecosystem of eHealth systems and services as well as their potential interdependencies with other sectors.

Your role in the experts group would be:

- To contribute to relevant position and policy papers on security topics in Healthcare;
- To exchange knowledge with other participants and ensure the convergence of current and future cyber security efforts;
- To participate with priority in related workshops organised by ENISA or other important stakeholders of the community;
- To discuss on the approaches taken towards protecting eHealth systems and services (policy, good practices, standardisation…)

Members of the ENISA eHealth Security Experts Group have the following benefits:

- Orient and review ENISA studies by sharing their experience on current threats and good practices;
- Attend (possibly) ENISA workshops or other related events related to the security and resilience of the Healthcare sector;
- Exchange information with other experts from the sector in a trusted manner;
- Contribute directly to ENISA's work with the possibility to express their opinion on current and future policy.

3. EHEALTH SECURITY EXPERT 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 eHealth;

- Experience in the area of eHealth security and resilience and knowledge of relevant sector-specific guidelines and standards;
- Technical background on cyber security in eHealth.;
- 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 in eHealth, sector and geographic coverage is taken into account;
- Limited number of experts in order to efficiently interact in achieving desired outcomes; (maximum 20 members and 5 alternate members);
- Interest or motivation of the Expert in regard to the technical or policy area;
- General background of the Expert in the technical or policy area;
- Gender balance.

4. ADMINISTRATIVE INFORMATION

4.1 APPROACH / WORKING METHODS

The structure of the experts 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. ENISA is the Chair of this Experts Group but agenda items are commonly agreed.

The main means of interaction of the eHealth 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 eHealth 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 eHealth Security Experts Group activities will not NOT be reimbursed by ENISA. Participation is based on voluntary work.

The travelling expenses of the eHealth Security Experts Group related to a potential physical meeting will not 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 eHealth Security Experts Group members.

4.3 DATA PROTECTION

Personal data of participants in Informal Expert Groups will be processed in accordance Regulation 2018/1725[1] on the protection of personal data by EU institutions and bodies.

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. 2018/1725, 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 eHealth 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.

---

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