

Terms of Reference for the Transport Resilience and Security Expert Group (TRANSSEC)

ENISA launches this Call for Participation to invite experts in security of different sections of the Transport sector to participate in its expert group.

TRANSSEC is an evolution of the existing ENISA TRANSSEC Experts Group (call 2016) which aims at gathering experts from the Transport sector to exchange viewpoints and ideas on cyber security threats, challenges and solutions. It is the intent of ENISA for this group to produce specialised workstream focusing on specific sub-sectors of transport, namely Air, Rail and Water Transport with the possibility of eventually establishing one or more specialised individual Expert Groups.

1 Background

ENISA creates this expert group to cover security and resilience of Transport systems as they undergo a digital transformation built around a plethora of interconnected devices and systems that facilitate automation and intelligent decision-making.

The threats and risks associated with the digital transformation of the Transport sector are manifold and have a potential impact on citizens' safety, health and privacy in addition to the availability of the critical transport services themselves. Hence, it is important to understand the entire ecosystem, identify what needs to be secured and develop specific security measures to protect Transport from cyber threats.

TRANSSEC is an information exchange platform that brings together experts to ensure security and resilience of the Transport sector in Europe.

Experts of the TRANSSEC shall have technical background expertise and direct exposure on one or more of the following:

- Operators and infrastructure owners of Transport systems with an interest in cyber security in one or more of the following sub-sectors
 - Air Transport (e.g. Air carriers, Airports, Traffic Management control operators etc.)
 - Rail Transport (e.g. Infrastructure managers, service facilities etc.)
 - Water Transport (e.g. Water Transport Companies, Ports, Vessel Traffic Services etc.)
- Manufacturers or integrators of Transport systems with a focus on cyber security;
- Suppliers and developers of transport hardware and/or software with a focus on cyber security;
- Associations and not-for-profit organisations involved in Transport security;
- Relevant authorities, academia, standardisation bodies and policy makers directly involved in the above topics.

2 Objectives

With the objective of making Transport 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 TRANSSEC shall contribute to enhance the current level of cyber security of the Transport by sharing their expertise on current threats, challenges and solutions.



The scope of TRANSSEC is focused on securing the entire ecosystem of Transport infrastructure in the Air, Rail and Water Transport sub-sectors 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 Transport;
- 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;
- Discuss other on the approaches taken towards protecting Transport infrastructures and services (policy, good practices, standardisation...)

Members of TRANSSEC 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 related to the security and resilience of the Transport sector;
- 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 TRANSSEC 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 Air or Rail or Water Transport;
- Experience in the area of Transport infrastructure security and resilience and knowledge of relevant sector-specific guidelines and standards. An emphasis on cyber security for safety would be a plus;
- Technical background on cyber security in Transport critical infrastructure, intelligent transport systems, smart logistics, assorted Hardware/Software components and systems etc.;
- 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 Transport, 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 per specialised workstream or resulting sub-sector expert group);
- 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 website¹. 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 TRANSSEC 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.

The intent is for the TRANSSEC Expert Group to be split in specialised workstreams, individually covering the Air, Rail and Water Transport sub-sectors. The aforementioned Approach/Working Methods will apply on a per specialised workstream basis should one or more such workstreams be created.

4.2 Organisational modalities

A long term commitment by the group members is desirable. The contribution of each member of TRANSSEC 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 TRANSSEC activities will NOT be reimbursed by ENISA. Participation is based on voluntary work.

The travelling expenses of TRANSSEC members 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 TRANSSEC members. With the approval of the members, on the meetings could be invited external people to provide specific knowledge.

¹ <https://resilience.enisa.europa.eu/intelligent-public-transport-security-and-resilience>

4.3 Data protection

Personal data of participants in Informal Expert Groups will be processed in accordance with Regulation 2018/1725² on the protection of natural persons with regard to the processing of personal data by the Union 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.

Information on Informal Expert Groups and their composition will be disclosed by the Agency on its website. Information disclosed includes the name of the Informal Experts Group, the scope, names of all participants and affiliation if acting on behalf of an entity other than themselves.

4.5 Duration of this Call

This Call for Expression of Interest inviting experts to the ENISA TRANSSEC Expert 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.

² 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