CYBERSECURITY FOR ARTIFICIAL INTELLIGENCE

CALL FOR APPLICATIONS FOR THE SELECTION OF MEMBERS OF AN ENISA AD HOC WORKING GROUP

1. INTRODUCTION

AI is an emerging concept facilitating intelligent and automated decision-making and thus becoming a prerequisite to the deployment of IoT and Industry 4.0 scenarios, as well as other application areas. Whereas undoubtedly beneficial, one should not sidestep the fact that AI and its application on automated decision making – especially in safety critical deployments such as in autonomous vehicles- might open new avenues in manipulation and attack methods, while creating new privacy challenges. A number of ongoing H2020 projects are looking at the interlinks between AI and cybersecurity.

When considering security in the context of AI, one needs to consider that AI can be exploited to manipulate the expected outcomes, but also that AI techniques can be utilised to support security operations. Before considering using AI as a tool to support cybersecurity, it is **essential to understand what needs to be secured and to develop specific security measures to ensure that AI itself is secure and accordingly this is one of the areas on which ENISA will initially focus.**

ENISA's WP2020 Output O.1.1.3 on Building knowledge on Artificial Intelligence Security and the **EC White Paper on Artificial Intelligence**[1] have brought about the need for ENISA to look into the topic of Artificial Intelligence (AI) Cybersecurity (mostly from the perspective of securing AI, but also looking into the different aspects of AI and cybersecurity as mentioned above) in a holistic and coordinated manner. In particular, the mapping of the AI Threat Landscape (AI TL) using threat assessment has emerged as an important topic, as well as the drawing of proportionate security measures and recommendations. ENISA will take stock of existing

[1] See EC White Paper on Ai under consultation at: https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

initiatives and studies that are ongoing in the area of AI cybersecurity such as the results of EU projects in this area (H2020) and will avoid duplication of efforts, rather focus on provide harmonized view of ongoing works.

2. BACKGROUND OF THE AD HOC WORKING GROUP

As stipulated in Regulation (EU) 2019/881[2], Art. 20, the Executive Director of the EU Agency for Cybersecurity may set up ad hoc working groups composed of experts, including experts from the Member States' competent authorities, where necessary and within ENISA's objectives and tasks. Ad hoc working groups provide ENISA with specific advice and expertise. Prior to setting up an ad hoc working group, the Executive Director of ENISA shall inform the agency's Management Board.[3]

The members of the ad hoc working groups are selected according to the highest standards of expertise, aiming to ensure appropriate balance according to the specific issues in question, between the public administrations of the Member States, the Union institutions, bodies, offices and agencies, and the private sector, including industry, users, and academic experts in network and information security.[4]

ENISA's WP2020 Output O.1.1.3 on Building knowledge on Artificial Intelligence Security and the EC White Paper on Artificial Intelligence[5] have brought about the need for ENISA to look into the topic of Artificial Intelligence (AI) Cybersecurity (mostly from the perspective of securing AI, but also looking into the different aspects of AI and cybersecurity as mentioned above) in a holistic and coordinated manner.

Along these lines, ENISA seeks to interact with a broad range of stakeholders for the purpose of collecting input on a number of relevant aspects including but not limited to: AI security; AI cybersecurity challenges; AI asset taxonomy; dataset security; AI Cyber Threat Intelligence; AI threat landscape; AI risk management; AI algorithmic security; data security in relation to AI; sectorial AI expertise; security measures; recommendations; applicable standards; relevant EU policies; AI trustworthiness; explainability and verification of AI; related technological fields.

The membership to these groups is foreseen to pursue broad, interdisciplinary representation across stakeholders' communities.

3. SCOPE OF THE AD HOC WORKING GROUP

The scope of this ad hoc working group is to advise ENISA in developing an AI cybersecurity threat landscape and other tasks related to AI cybersecurity.

Key tasks of this ad hoc working group include:

- advising ENISA on developing asset taxonomy and threat landscape for Artificial Intelligence using risk management methodology;
- advice on mitigating AI risks, including advice on specific use cases and application scenarios in the field;

[2] Article 20(4) of Regulation (EU) 2019/881.
3 Article 49(4) of Regulation (EU) 2019/881.
4 Recital 59 of Regulation (EU) 2019/881,
[5] See https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

- review of related ENISA deliverables;
- advising ENISA on related security measures and recommendations;
- generally advising ENISA in carrying out its tasks in relation to Artificial Intelligence cybersecurity.

The preliminary estimate of the duration of the ad hoc working group is for up to one (1) calendar year from the kick off date of this working group; extension of the mandate of this ad hoc working group is possible, should the scope of the work is not completed in one (1) year.

4. APPOINTMENT OF MEMBERS

The members of the ad hoc working groups shall be appointed by the Executive Director of ENISA from a list of suitable applicants duly selected in line with this call.

The appointment will be done for a period equal to the duration of the working group.

The selection of members is based on a personal capacity or for the purpose of representing particular interests that generally serve a public goal and they have a clear demonstrable skillset in such areas as AI security AI cybersecurity policy; dataset security; AI cybersecurity challenges; AI asset taxonomy; AI threat landscape; AI risk management; AI Cyber Threat Intelligence;AI algorithmic security; sectorial AI expertise; data security in relation to AI; security measures; recommendations; applicable standards; relevant EU policies; AI trustworthiness; explainability and verification of AI; related technological fields.

The members of this ad hoc working group may be reimbursed for their expenses to participate in the meetings according to the ENISA Reimbursement rules.

Besides members of the ad hoc working group, ENISA is likely to establish a reserve list, in accordance with the same conditions that apply to members, who shall be called to replace any members indisposed due to reasons stated below.

Members who are no longer willing or no longer capable to contribute effectively to the group's deliberations, who in the opinion of ENISA do not comply with the conditions set out in Article 339 of the Treaty on the functioning of the European Union or who resign, shall no longer be invited to participate in any meetings of the Group and may be replaced for the remaining duration of the ad hoc working group.

Organisations and public entities, such as EU bodies, offices or agencies and international organisations, may be granted an observer status; organisations and public entities appointed as observers shall nominate their representatives. Observers and their representatives may be permitted by the Chair to take part in the discussions of the group and provide expertise. Their representatives generally cover their own expenses.

ENISA staff will be designated as Chair and Secretariat of the ad hoc working group.

An ad hoc working group may be supported by up to three rapporteurs who can assist with editorial, document management and other associated tasks. Rapporteurs are selected from among the members of the ad hoc working group; they may be remunerated for their services and they may be reimbursed for their expenses to participate in the meetings according to the ENISA Reimbursement rules.

ENISA will propose to the ad hoc working group a set of draft rules of procedure to be adopted as appropriate.

The membership of an ad hoc working group is generally limited to fifteen (15) members. Additionally, representatives of the various organisations and bodies, mentioned above can join meetings as observers.

In principle, the ad hoc working group shall convene in ENISA premises or as otherwise decided on a proposal of the Chair. The bulk of the work can be carried out remotely; conference calls or video conferencing are permitted and encouraged; support and planning will be provided by ENISA as appropriate.

The members of the ad hoc working group, as well as invited experts and observers, are subject to the obligation of professional secrecy, which by virtue of the Treaties and the rules implementing them applies to all members of the institutions and their staff, as well as, by analogy, to the Commission's rules on security regarding the protection of Union classified information, laid down in European Commission Decisions (EU, Euratom) 2015/44310 and 2015/444.[6]

5. TRANSPARENCY

The members of the ad hoc working group (including rapporteurs) shall make a confidentiality and an absence of conflict of interest statement. Observers, invited experts etc. have no such obligation. Ad hoc working groups are subject to the conditions of Regulation (EC) No 1049/2001.[7]

6. PERSONAL DATA PROCESSING

Personal data shall be collected, processed and published in accordance with Regulation (EU) 2018/1725[8]. For further information, please refer to the data protection notice that is available as a separate document with the call.

7. REMUNERATION OF RAPPORTEURS

Each selected member acting as rapporteur may be remunerated with a fixed fee of €450 per person per day. Remunerated services require withholding the corresponding amount of tax as per EU Member States' legislation in force; ENISA fully complies with this requirement. A cap of €15000 (annual aggregate that includes any and all work items commissioned by ENISA, including costs) is applied to remunerations per person per calendar year by direct award for all activities an expert is involved with ENISA, in line with the ENISA Financial Regulation.

Rapporteurs may decide to refrain from collecting remuneration on the basis of personal or professional considerations; in this case they remain eligible to apply.

6 Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53).
7 Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents. Exceptions are intended to protect public security, military affairs, international relations, financial, monetary or economic policy, privacy and integrity of the individual, commercial interests, court proceedings and legal advice, inspections/investigations/audits and the institution's decision-making process.
8 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 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.

8. REIMBURSEMENT OF MEMBERS

Members of an ad hoc working group may be reimbursed for their travel and subsistence expenses. If a member is from a location other than the location required for the provision of services or place of meeting, the following expenses are then eligible:

1. Travel expenses (economy class flight or 1st class train – whichever is more cost effective) from the European country/city in which the contractor is officially registered to another European city.
2. A "per diem" applicable to the country in which the meeting will take place. This allowance is set by the European Commission (download the latest rates from website (http://ec.europa.eu/comm/europeaid/perdiem/index_en.htm) and it covers all daily living expenses including hotel, meals, local travel etc.
3. No other claims for living or transportation costs will be accepted.

Members may select to refrain from being reimbursed on the basis of personal or professional considerations; in this case they remain eligible to apply.

Observers are neither remunerated nor reimbursed, except in duly justified cases, to be determined by the Executive Director of ENISA.

9. APPLICATION PROCEDURE

Individuals interested are invited to submit their application to ENISA via the dedicated section on the ENISA web site. Applications must be completed in one of the official languages of the European Union. However, applications in English would facilitate the evaluation procedure. If another language is used, it would be helpful to include a summary of the CV and/or the application in English. An application will be deemed admissible only if it is submitted by the deadline.

9.1 DEADLINE FOR APPLICATION

The duly completed applications must be submitted by **18:00 (CET time) on 15th of April 2020**. The date and time of submission will be established on the website upon submission of an application.

10. SELECTION CRITERIA

ENISA will take the following criteria into account when assessing applications:

- Relevant competence (e.g. technical, legal, organisational or a combination thereof) and experience in the area of Artificial Intelligence cybersecurity and/or in other areas of relevance for the purpose of providing advice on Artificial Intelligence cybersecurity, such as the knowledge of the ICT market, developments as regards the cyber threat landscape, knowledge and experience in big data/dataset security, algorithmic security, software/hardware security, sectorial AI expertise and other relates cybersecurity facets.
- Ability to deliver technical advice at the tactical level, including those of scientific or technical nature, on issues relevant to Artificial Intelligence cybersecurity, including in the above-mentioned areas of relevance for this purpose.
- Good knowledge of English allowing active participation in the discussions.

11. SELECTION PROCEDURE

The selection procedure shall consist of an assessment of the applications performed by ENISA as appropriate against the selection criteria mentioned above in this Call, followed by the establishment of a list of the most suitable applicants and concluded by the appointment of the members of the ad hoc working group by the Executive Director of ENISA.