CYBER THREAT LANDSCAPES

CALL FOR APPLICATIONS FOR THE SELECTION OF MEMBERS OF ENISA AD HOC WORKING GROUP ON CYBER THREAT LANDSCAPES

1. INTRODUCTION

The cyber threat landscape is constantly evolving. Both policy makers and practitioners need up to date and accurate information on the current threat landscape, supported by threat intelligence. To respond to this need, the EU Agency for Cybersecurity (ENISA) Threat Landscape has been published on an annual basis over the years. It is based on publicly available data and provides an independent view on observed threats, threat agents, threat trends and attack vectors. ENISA aims at building on its expertise and enhancing this activity so that its stakeholders receive relevant and timely information for policy, decision-making, and applying security measures, as well as in increasing knowledge and information for specialised cybersecurity communities or on new technologies. Its added value lies in offering updated information on the dynamically changing cyber threat landscape that can be used to support risk mitigation and proactively respond to future challenges.

ENISA's Work Programme 2021 Output O.8.2 highlights the need for ENISA to revisit the topic of threat landscape(s). Following the revised form of the ENISA Threat Landscape Report 2020, ENISA wishes to continue and further improve this flagship report. In particular, ENISA seeks to provide targeted as well as general reports, recommendations, analyses and other actions on future cybersecurity scenarios and threat landscapes, supported via a clear and publicly available methodology and IT tools. By establishing a methodology to develop threat landscapes, the Agency aims to set a baseline for the transparent and systematic delivery of horizontal, thematic and sectorial cybersecurity threat landscapes.

ENISA will take stock of existing initiatives and studies that are ongoing in this area, such as the results of EU initiatives or other threat landscapes and will avoid duplication of efforts.

2. BACKGROUND OF THE AD HOC WORKING GROUP

As stipulated in Regulation (EU) 2019/881[1], Art. 20(4), 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.[2]

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.[3]

ENISA's WP2021 Output 8.2 aims at enabling ENISA to provide targeted as well as general reports, recommendations, analyses and other actions on future cybersecurity scenarios and threat landscapes. This includes the delivery of the annual flagship ENISA Threat Landscape (ETL), as well as a new, clear and publicly available methodology for threat landscapes.This will allow for the systematic monitoring of ETL on a yearly basis. It will also set the methodological foundations for drawing future cybersecurity threat landscapes (also thematic or sectorial), and for the specification and development of IT tools to support said methodology and future ETL related outputs.

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:

- cyber threat intelligence (collection, analysis, production, or consumption);
- digital forensics;
- risk management;
- threat landscape;
- threat taxonomy;
- sectorial threat expertise;
- incident handling;
- incident response;
- cyber attack vectors;
- attack scenarios;
- threat actors' profiling;
- threat awareness;
- media and social media monitoring;
- recommendations;
- applicable standards, tools and methods;
- relevant EU policies and initiatives.

[1] Article 20(4) of Regulation (EU) 2019/881.
[2] Article20 (4) of Regulation (EU) 2019/881.
[3] Recital 59 of Regulation (EU) 2019/881.

Whereas these aspects are of horizontal nature in terms of mapping the cybersecurity threat landscape, for the purpose of thematic (e.g. AI, 5G) or sectorial (e.g. NISD sectors) threat landscapes, a relevant deep technical understanding of the technological fields or sectors that require threat assessment is beneficial.

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 designing, updating and reviewing the methodology for creating cyber threat landscapes, including the annual ENISA Threat Landscape.

Key tasks of this ad hoc working group include:

- advice on maintaining and extending a cyber threat taxonomy;
- advice on analyzing cyber threat intelligence;advice on designing threat landscape(s) using risk management methodologies;
- advice on the selection of top threats per specific time period;
- assistance on the analysis of identified threats;
- advice on assessing the wider impact of cyber incidents;
- advice at the tactical level on issues relevant to cyber threat landscapes and intelligence, including those of scientific or technical nature;
- review of related ENISA deliverables;
- advice on improving future ENISA Threat Landscapes; and
- generally advising ENISA in carrying out its tasks in relation to cyber threat landscapes and cyber threat intelligence; this ad hoc advice could take the form of reports/briefs drafted from the members of the ad hoc working group on specific subjects.

To perform these tasks, members of the ad hoc working group are expected to participate in the meetings of the group, and to provide written feedback to ENISA between meetings and upon request (survey)..

A minimum of 4 meetings per year are foreseen and a minimum of two days of active engagement. The preliminary estimate of the duration of the ad hoc working group is for up to two (2) calendar years 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 two (2) years.

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 cyber threat intelligence (collection, analysis, production, or consumption), forensics, risk management, threat landscape, threat taxonomy, sectorial threat

expertise, incident handling, incident response, cyber attack vectors, attack scenarios, threat actors' profiling, threat awareness, media and social media monitoring, recommendations, applicable standards, applicable tools and methods, relevant EU policies and initiatives, technological fields and/or sectors that require threat assessment.

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 appoint a reserve list, in accordance with the same conditions that apply to members, who shall be called to replace any members who are absent or otherwise indisposed.

Members who are 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 rapporteur(s), who are selected from among the members of the ad hoc working group.

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 case of a member's unavailability, disqualification or resignation the chair of the ad hoc working group can appoint a member (or members) from the reserve list, to replace any members who are indisposed. The new member(s) will be appointed for the remaining of the term of the ad hoc working group.

In principle, the ad hoc working group shall convene online or 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.[4]

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.[5]

6. PERSONAL DATA PROCESSING

Personal data shall be collected, processed and published in accordance with Regulation (EU) 2018/1725[6]. For further information, please refer to the data protection notice that is available as a separate document with the call.

7. RAPPORTEURS

A working group may designate Rapporteur(s) from among its members who shall ensure that draft reports or opinions are prepared, if necessary within a set of time period. The work of the Rapporteur is terminated when the Working Group adopts the report or opinion. Each selected member acting as rapporteur may be remunerated,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.

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 (https://eeas.europa.eu/archives/docs/jobs/docs/20140108/list_per_diem_en.pdf) 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.

4 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).
5 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.
6 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.

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 12h00 EET (Athens time) on 29th of March 2021. 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 cybersecurity, and/or in other areas of relevance for the purpose of performing the tasks of the ad hoc working group.
- Relevant competence and experience in designing and producing cyber threat landscapes and providing advice on cyber threat landscapes and intelligence.
- Ability to deliver technical advice at the tactical level, including those of scientific or technical nature, on issues relevant to cyber threat landscapes and intelligence.
- Experience in sectorial threat mapping would be beneficial to have.
- Good knowledge of English allowing active participation in the discussions, and in the drafting of related deliverables.

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.