

AWARENESS RAISING IN ENISA

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

To advise ENISA in designing, developing, launching and evaluating cybersecurity awareness raising campaigns and support creating and disseminating promotional material for ensuring cybersecurity best practices adoption.

1. INTRODUCTION

Cybersecurity incident rates show that cybersecurity still remains an unknown word to great part of the European population¹. The new reality derived from the pandemic created virtual activities for everyone; from students attending virtual classes to elderly benefiting from remote care services. Whether cybersecurity is a crucial component in all these virtual interaction remains an open question. The most recent cybersecurity incident reports² and threat landscape³ indicate that large scale phishing campaigns still remain the most popular and efficient attack method, as it requires the least sophistication and in parallel achieves great impact. The importance of greater cybersecurity awareness and the need for a basic cyber hygiene culture has become all the more important. To respond to this need, ENISA draws on a structured approach in raising cybersecurity awareness and education. ENISA aims at building on its expertise and enhancing this activity so that its stakeholders and the overall European community obtain an elevated level of cybersecurity hygiene and awareness, and eventually change behaviour towards

¹ https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

² <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents>

³ <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends>



prominent cybersecurity attacks. It's added value lays in promoting and disseminating the existing expert knowledge that can pave the way towards a trusted and cyber secure Europe.

Regulation (EU) 2019/881⁴ Article 10 stipulates ENISA's activities with regards to awareness raising and education. Moreover, ENISA's SPD 2021-2022⁵ Activity 9 highlights the need for dedicated activities towards awareness raising and promotion. Under this activity ENISA plans on drawing a stakeholder's strategy, identifying the cybersecurity needs and gaps, and design and develop targeted awareness raising and promotion campaigns to enhance the cybersecurity posture of European community. Apart from the ENISA flagship, the European Cybersecurity Month, ENISA plans on launching a full fledged cybersecurity awareness plan based on which several awareness raising campaigns will be launched. Similarly, ENISA will support cybersecurity in education not only by enhancing the Higher Education Database⁶ but also by contributing to the development of a the cybersecurity skills framework. ENISA will also investigate further investment in cybersecurity through the Digital Education Action Plan.

In this effort, ENISA will take stock of existing programmes and initiatives that are ongoing and establish synergies for example with other European Institutions and recognised bodies, avoiding duplication of activities.

2. BACKGROUND OF THE AD HOC WORKING GROUP

As stipulated in Regulation (EU) 2019/881⁷, Art. 20 (4), the Executive Director of the EU Agency for Cybersecurity may set up ad hoc working groups composed of experts 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.⁸

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.⁹

ENISA's SPD2021 Activity 9 aims at enabling ENISA to organise activities that will raise cybersecurity awareness and promote cybersecurity practices and organise targeted awareness campaigns and bolster already existing initiatives. This includes the delivery of the annual flagship ENISA European Cybersecurity Month, spanning its activities throughout the entire year, as well as designing targeted campaigns deriving from the new stimulating awareness raising plan. This plan will be built together with the related stakeholders and will result in an annual awareness calendar. This will also set the foundation for the promotion and take up of cybersecurity best practices and recommendations, with a potential impact on how citizens/consumers/users think and act about cybersecurity. .

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: awareness raising

⁴ Article 10 of Regulation (EU) 2019/881. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) OJ L 151, 7.6.2019, p. 15–69

⁵ <https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2021-2023/>

⁶ <https://www.enisa.europa.eu/topics/cybersecurity-education/education-map>

⁷ Article 20(4) of Regulation (EU) 2019/881.

⁸ Article 20(4) of Regulation (EU) 2019/881.

⁹ Recital 59 of Regulation (EU) 2019/881,



campaigns related to cybersecurity; designing and developing AR campaigns; measuring impact; measuring outreach; principles for promotional material; designing educational material; stakeholder management principles; stakeholder management tooling; platforms and tools for promotional activities; media and social media monitoring; recommendations; communication strategy principles; relevant EU initiatives.

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, developing, launching and evaluating cybersecurity awareness raising campaigns and support creating and disseminating promotional material for ensuring cybersecurity best practices adoption.

Key tasks of this ad hoc working group include:

- Advise on designing and developing cybersecurity awareness raising material and campaigns;
- Advise on developing awareness raising programmes and processes;
- Advise on evaluating and measuring the impact of a cybersecurity campaigns;
- Advise on identifying stakeholders and their needs on cybersecurity awareness;
- Advise on selection of principles and methods for developing and implementing promotional campaigns;
- Assist on the development of educational material;
- Assist on assessing the tools and channels to be used for promotional activities;
- Review of deliverables/documentation deriving from the ENISA projects;
- Advise on improving future ENISA awareness raising campaigns; and
- Generally advising ENISA in carrying out its tasks in relation to cybersecurity awareness and promotional material development.

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. Annually, a total workload of 6 working days is foreseen which would include monthly conference calls, 1 or 2 physical meetings and review of documentation (2 – 3 requests per 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 cybersecurity awareness raising, developing and maintaining stakeholder strategy, stakeholders management, promotional material development, communication strategy implementation and development, media and social media monitoring, impact and daily monitoring and measurement, educational material design and development, managing promotional tools and channels, awareness plan and calendar.

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 can assist with editorial, document management and other associated tasks. Rapporteurs 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. 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. 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 2015/444.¹⁰

¹⁰ 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. 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 1049/2001.¹¹

6. PERSONAL DATA PROCESSING

Personal data shall be collected, processed and published in accordance with Regulation (EU) 2018/1725¹². For further information, please refer to the data protection notice that is available as a separate document with the call.

7. REMUNERATION OF RAPPOREURS

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 (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.

¹¹ 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.

¹² 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.



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. Applications should be sent to the dedicated mailbox: Awareness@enisa.europa.eu

9.1 DEADLINE FOR APPLICATION

The duly completed applications must be submitted by 12h00 EET (Athens time) on 9th of April 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 awareness raising, and/or in other areas of relevance for the purpose of performing the tasks of the ad hoc working group, and of designing and organising cybersecurity awareness raising campaigns.
- Relevant competence (e.g. professional experience) or/and academic background on the field of cybersecurity awareness raising and education, with a link to communication outreach and dissemination.
- Ability to deliver technical advice at the tactical level, including those of scientific or technical nature, on issues relevant to cybersecurity best practises and building educational material related to those.
- Good knowledge of English allowing active participation in the discussions and good EN writing skills.
- Advantageous: relevant experience in designing and implementing citizen and/or consumer wide awareness raising campaigns (not directly linked to cybersecurity).

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 a reserve list, and concluded by the appointment of the members of the ad hoc working group by the Executive Director of ENISA.