ENSEC WG TOR

CALL FOR APPLICATIONS FOR THE SELECTION OF MEMBERS OF AN ENISA AD-HOC **WORKING GROUP** IN ENTERPRISE SECURITY

To advise ENISA in building knowledge and expertise on cybersecurity aspects of small and medium size enterprises and to assist in building the know-how to tackle cybersecurity issues

1. INTRODUCTION

Accounting for more than half of Europe's GDP, SMEs are a key driver of innovation and growth across the Union. Their well-being is vital to both the economy and society. The pandemic has put an incredible stress on these businesses. SMEs are not only navigating a new digital realm where employees work from home and business is increasingly conducted online, but they are also facing more advanced and targeted cyber threats.

Small and medium-sized enterprises (SMEs) are the backbone of EU's economy. They represent 99% of all businesses in the EU and employ around 100 million people. There were slightly more than 25 million SMEs in the EU-28 in 2018. . Thus they play significant role in society and business and every National Cybersecurity Strategy (NCSS) should aim at creating cyber-literate SMEs.

As part of its mission to achieve a high common level of cybersecurity across the Union and be a centre of expertise on cybersecurity, the EU Agency for Cybersecurity – ENISA intends to

increase SMEs cybersecurity capacity by performing capacity building activities such as developing and maintaining cybersecurity good practices, tools, and guidelines for SMEs, as well as raise their cybersecurity awareness on common threats and risks to help them increase their cybersecurity posture in the online environment and contact business online safely.

The capacity building activities to increase the cybersecurity of SMEs are expected to be taking place for the next two to threee years and will cover: Cybersecurity good practices, development of cybersecurity tools, developing of awareness activities, providing online trainings, all with the aim of increasing the cybersecurity posture of European SMEs.

The work on SMEs is expected to accomodate both **technical** and **organisational** elements but also take into account **policy** aspects and **capacity-building** activities. The work besides increasing the cybersecurity of SMEs, will also serve as a source of information that will helps EU Member States and the European Commission (EC) to base appropriate policy actions, promote a high common level of security of networks and information systems across the Union, but also to instigate identified areas for capacity building, training and awareness raising activities for this community.

ENISA's Work programme 2021 Output 3.1 is to Aassist MS to develop NCSS has brought about the need for ENISA to look into the topic of SMEs, empower this community and share knowledge on their cybersecurity aspects across the EU. Moving towards this direction ENISA aims to develop internal knowledge of the needs and requirements of SMEs and equip them with the necessary means to become cyber resilient.

2. BACKGROUND OF THE AD HOC WORKING GROUP

As stipulated in Regulation (EU) 2019/881[1], 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.[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]

Along these lines, ENISA seeks to interact with a stakeholders representing the EU MS for the purpose of collecting input on a number of relevant aspects regarding SMEs including but not limited to:

- Cybersecurity policy;
- Technical and organisational security measures;
- Market aspects of cybersecurity (e.g. standards, best practices, security-by-design, standards, etc.),
- Capacity building, awareness raising, risk management,

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

- Cybersecurity threats and risk and their mitigation measures

3. SCOPE OF THE ENSEC WORKING GROUP

The scope of this ad hoc working group is to advise ENISA in building knowledge and expertise on cybersecurity aspects of small and medium size enterprise and help in building the know-how to tackle cybersecurity issues.

Key tasks of this ad hoc working group include:

- Advising ENISA on developing knowledge on the issues and needs of SMEs.
- Advising ENISA on developing best practices on how SMEs should tackle cyber security issues and risk;
- Advising ENISA on awareness activities for SMEs and potential trainings that could developed to help raising their cybersecurity posture and know-how.
- Advising ENISA on presentation, functionality of the developed material such as tools, reports and other related material.
- Reviewing and validating related ENISA deliverables.
- Advising ENISA in carrying out its tasks in relation to this topic.
- Participating in workshops and teleconferences for the purpose of the above activities.

The ENISA Enteprise Security (ENSEC) ad hoc working group will focus on cybersecurity of small and medium enterprise (SME), as they often lack necessary know-how, finance and manpower to tackle complex cybersecurity issues.

ENSEC will ensure the scope of work will be suitable to SME's needs, and the final outcome readily useable. As most of SMEs are actually micro-SMEs, i.e. those with up to 10 employees, the cybersecurity advice needs to be delivered in a straightforward and simple-to-follow step by step instructions. ENISA National Liasion Officer (NLO) network will provide necessary feedback from Member States, while individual businesses will keep eye on the deliverable's utility and comprehensibility.

The preliminary estimate of the duration of the ad hoc working group is for up to **three (3)** 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 three (3) years.

Annually, a total workload of 6 working days for three years is foreseen, which would include a monthly conference call and one or two annual meetings.

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 members of the ENSEC will represent particular interests of SMEs, their respective EU Member State, or EU Institution. The ENSEC members that will be appointed must have a clear work-related skillset in such areas as cybersecurity policy; market aspects of cybersecurity (e.g.

certification, security-by-design, standards etc.), capacity building activities such as risk management, cybersecurity awareness, technical and organisational measures, cybersecurity threats/risks and their mitigation measures;National Cybersecurity Strategies; etc.

Besides members of the ad hoc working group, ENISA is will 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. In such case replaced replacement can be appointed by the relevant EU MS or Institution or selected by the chair of the ad hoc working group from the reserve list , 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.

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

The membership of the working group may vary over its duration depending on the interest of the relaevant EU MS and Institutions. In any case though, it shall not exceed 20 members (up to 10 for MS' national authorities and 10 industry representatives (SMEs)). The ENSEC may include also other experts, ad personam. The role of an observer may be assigned to the persons who just want to follow up the proceedings of the group, e.g. additional individuals from EU MS and/or Insitutions, EU Associations that represent SMEs, etc.

In principle, the ad hoc working group shall might 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 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. Chatam house rules might apply in meetings to encourage inclusive and open dialogue in meetings of the group.

5. TRANSPARENCY

The members of the ENSEC working group 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.[4]

4 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. PERSONAL DATA PROCESSING

Personal data shall be collected, processed and published in accordance with Regulation (EU) 2018/1725[5]. For further information, please refer to the data protection notice that is available as a separate document with the call.

7. REIMBURSEMENT OF MEMBERS

Members of the ENSEC 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.

8. APPLICATION PROCEDURE

Individuals interested are invited to submit their application to ENISA via the dedicated section on the ENISA website. 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.. Applications must include at least the following information:

- MSs; National Authority information:
  - Country, Organisation, Name/Surname
- Industry representatives (SMEs) information:
  - Country, Organisation, Name/Surname, current role, brief description (1-2 paragraphs) on the interest for ENISA's work on SMEs including any ideas, size of the organisation (1-250 employees), a brief CV (if available)

8.1 DEADLINE FOR APPLICATION

The duly completed applications must be submitted by 12h00 EEST (Athens time) on 20th May 2021. The date and time of submission will be established on the website upon submission of an application.

5 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.

An application will be deemed admissible only if it is submitted by the deadline.

9. SELECTION CRITERIA

ENISA will take the following criteria into account when assessing applications for two types of candidates:

For EU MSs' public authority representatives:

- Relevant competence (e.g. professional experience) or/and academic background in the field of cybersecurity in particular technical, legal, organisational or a combination thereof and experience in the area of capacity building in cybersecurity, and/or in other areas of relevance for the purpose of performing the tasks of the ENSEC working group, and of developing cybersecurity guidelines for SMEs.
- Ability to deliver advice at the technical, operational and policy level, including issues relevant to cybersecurity best practises and building capacity building material related to those.
- Relevant knowledge of EU directives, EU national laws, and international laws concerning cybersecurity and more specifically laws and secondary laws, policy initiatives and communications on cybersecurity strategies, capacity building, knowledge management and raising awareness in cybersecurity.
- Good knowledge of English allowing active participation in the discussions and good EN writing skills.

For industry (SMEs) representatives:

- Relevant competence (e.g. professional experience) or/and academic background on the field of cybersecurity in particular technical, legal, organisational or a combination thereof and experience in the area of capacity building in cybersecurity, and/or in other areas of relevance for the purpose of performing the tasks of the ENSEC working group, and of developing cybersecurity guidelines for SMEs.
- Ability to deliver advice at the technical, operational and policy level, including issues relevant to cybersecurity best practises and building capacity building material related to those.
- Able to identify what are the needs of SMEs and raise awareness on cybersecurity best practices.
- Good knowledge of English allowing active participation in the discussions and good EN writing skills.
    Being a representative of an SME on the role of a CEO or the company's responsible for dealing with cybersecurity person or a representative that meets all above requirements (proof must be provided that the enterprise is either micro: 1-10 employees, small: 10-50 employees or medium size: 50-250 employees)

10. 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 ENSEC ad-hoc working group by the Executive Director of ENISA.