EU CYBERSECURITY CERTIFICATION

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

1. INTRODUCTION

Securing network and information systems in the European Union has been deemed as a key objective in an effort to keep the EU online economy functional and secure; it is evident that failure to do so could have far reaching consequences for European citizens and threatens to impact the trust of citizens, the industry and public administration alike. As the role of ENISA has been further bolstered by means of Regulation (EU) 2019/881,[1] the important task of cybersecurity certification calls for appropriate stakeholders' involvement and support.

The purpose of the EU cybersecurity certification framework under the Regulation (EU) 2019/881 is to provide a mechanism to establish and maintain trust and security on cybersecurity products, services and processes. Drawing up cybersecurity certification schemes at EU level aims at providing criteria to carry out conformity assessments to establish the degree of adherence of products, services and processes against specific requirements. Users and service providers alike, need to be able to determine the level of security assurance of the products, services and processes they procure, make available or use.

Cybersecurity certification requires the formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria, standards, and the issuing of a certificate indicating conformance; as such cybersecurity certification plays a key role in increasing trust and security in products, services and processes. Cybersecurity certification in the EU serves the purpose of providing notice and assurance to users about the level of conformity against stated requirements. EU cybersecurity certification schemes serve as the

1 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency on Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

vehicle to convey such requirements from the EU policy level to the industry service provision level and further to the users and conformity assessment bodies.

2. BACKGROUND AND TASKS

As stipulated in Regulation (EU) 2019/881, the EU cybersecurity certification framework lays down the procedure for the creation of EU cybersecurity certification schemes, covering ICT products, services and processes. Each scheme will specify one or more level(s) of assurance (basic, substantial or high), on the basis of the level of risk associated with the envisioned use of the product, service or process. To assist in establishing EU cybersecurity certification schemes, Regulation (EU) 2019/881 provides the modalities to set-up ad hoc working groups. The membership to these groups is foreseen to pursue broad representation across stakeholders' communities.

3. BACKGROUND OF THE AD HOC WORKING GROUP

In line with art. 20(4) of Regulation (EU) 2019/881, the Executive Director needs to set up ad hoc working groups for each candidate scheme, composed of experts, including the experts from the Member States' competent authorities. 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 broad range of stakeholders for the purpose of collecting input on the design of: an EU cybersecurity certification scheme; requirements; security goals; applicable standards; assurance level; requirements for conformity assessment; security evaluation criteria; rules for monitoring compliance; conditions to issue EU statement of conformity; aspects concerning vulnerabilities; aspects related to the valitidiy of a certificate; mutual recognition of certificates etc.[4]

4. SCOPE OF THE AD HOC WORKING GROUP

In accordance with article 48(2) of Regulation (EU) 2019/881 (hereinafter, Cybersecurity Act), ENISA seeks to assist the European Commission in the preparation of a candidate cybersecurity certification scheme to serve as a successor to the existing Senior Officials Group Information Systems Security (SOG-IS) Mutual Recognition Agreement (MRA).[5]

2 Article 49(4) of Regulation (EU) 2019/881.
3 Recital 59 of Regulation (EU) 2019/881,
4 As stipulated in art. 54 of Regulation (EU) 2019/881.
5 The scope of this group is laid out in a suitable Note of the European Commission to ENISA in line with Regulation (EU) 2019/881.

The scope of this ad hoc working group is to support ENISA in preparing the above-mentioned draft candidate cybersecurity certification scheme.

Key tasks of this ad hoc working group include a review of the existing achievements under SOGIS, the pre-qualification of elements that need to be included in a cybersecurity certification scheme, support the drafting of a scheme in line with the provisions of Regulation (EU) 2019/881 and generally support ENISA in carrying out its tasks in relation to the preparation of this draft candidate cybersecurity certification scheme.

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.

5. 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 public policy, market supervision, design of certification schemes, evaluation of software and hardware, vulnerability assessment, penetration testing, consumer protection, conformity assessment, accreditation, etc.

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 alternate members, 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.

Members of the European Cybersecurity Certification Group (ECCG) and of the Stakeholders Cybersecurity Certification Group (SCCG) may participate in the ad hoc working group as observers; they generally cover their own expenses.

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 elect up to two vice Chairs to support the Chair in her day to day tasks and activities.

An ad hoc working group may be supported by up to five 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 twenty (20) 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.

ENISA shall ensure interaction with the European Cybersecurity Certification Group (ECCG) throughout the lifespan of the ad hoc working group and other stakeholders (e.g. in the area of standardisation) who might need to be consulted during the working period.

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]

6. TRANSPARENCY

The members of the ad hoc working group (including vice chairs and 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]

7. PERSONAL DATA PROCESSING

Personal data shall be collected, processed and published in accordance with Regulation (EU) 2018/1725[8]. ENISA ensures that applicants' personal data are processed in accordance with 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. Personal data is processed according to a published policy. ENISA is supervised by EDPS,

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.

http://www.edps.europa.eu. For any further enquiries you may contact the ENISA Data Protection Officer at: dataprotection@enisa.europa.eu

8. 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.

9. 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.

10. 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.

10.1 DEADLINE FOR APPLICATION

The duly completed applications must be submitted by 12h00 EEST (Athens time) on 19 September 2019. The date and time of submission will be established on the website upon submission of an application.

11. 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 certification and/or in other areas of relevance for the purpose of providing advice on cybersecurity certification policy, such as the knowledge of the ICT market, developments as regards the cyber threat landscape, cybersecurity related conformity assessment procedures and standardisation, knowledge and experience in Common Criteria (ISO/IEC 15408).
- Ability to deliver technical advice at the tactical level, including those of scientific or technical nature, on issues relevant to cybersecurity certification, including in the above-mentioned areas of relevance for this purpose.
- Good knowledge of English allowing active participation in the discussions.

12. SELECTION PROCEDURE

The selection procedure shall consist of an assessment of the applications performed by ENISA and the Commission 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.