CALL FOR APPLICATIONS FOR THE SELECTION OF MEMBERS OF THE STAKEHOLDERS CYBERSECURITY CERTIFICATION GROUP

1. Introduction

Securing network and information systems in the European Union is essential to keep the economy running, to ensure prosperity and to protect against incidents, which can harm European citizens and business, and damage consumer trust in digital technologies.

To address this challenge, the Commission adopted on 13 September 2017 a wide-ranging set of measures aimed at strengthening cybersecurity, including the proposal for a Cybersecurity Act ('the Act') [1], which entered into force on 27 June 2019. The Act establishes an EU-wide voluntary cybersecurity certification framework.

In order to establish and preserve trust and security, Information and Communication Technologies (ICT) products, services and processes need to directly incorporate security features in the early stages of their technical design and development (security by design). Moreover, customers and users need to be able to ascertain the level of security assurance of the products and services they procure or purchase.

Certification, which consists of the formal evaluation of products, services and processes by an independent and accredited body against a defined set of criteria and standards and the issuing of a certificate indicating conformance, plays an important role in increasing trust and security in products and services. While security evaluations are quite a technical area, certification serves the purpose to inform and reassure purchasers and users about the security properties of ICT products and services. This is particularly relevant for new systems that make extensive use of digital technologies and which require a high level of security, such as e.g. connected and automated cars, electronic health, industrial automation control systems (IACS) or smart grids.

As set out in the Cybersecurity Act, the cybersecurity certification framework lays down the procedure for the creation of EU-wide cybersecurity certification schemes, covering ICT products, services and processes. Each scheme will specify one or more levels of assurance (basic, substantial and high), depending on the risk associated with the intended use of the product, service or process object of the scheme.

2. Background

In order to establish EU-wide certification schemes, the Cybersecurity Act provides for the setting-up of an appropriate governance system at EU level. This includes essential functions and tasks for the European Union Agency for Cybersecurity (ENISA) and the Commission, as well as key roles for national authorities and stakeholders to inform and assist ENISA and the Commission in this process.

[1] 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).

In particular, in order to help ENISA and the Commission facilitate consultation with relevant stakeholders, the Cybersecurity Act provides for the establishment of a Stakeholder Cybersecurity Certification Group ('the group').

In accordance with Article 22 of the Act, the the group shall:

(a) advise the Commission on strategic issues regarding the European cybersecurity certification framework;

(b) upon request, advise ENISA on general and strategic matters concerning ENISA's tasks relating to market, cybersecurity certification, and standardisation;

(c) assist the Commission in the preparation of the Union rolling work programme referred to in Article 47 of the Act;

(d) issue an opinion on the Union rolling work programme pursuant to Article 47(4); and

(e) in urgent cases, provide advice to the Commission and the European Cybersecurity Certification Group on the need for additional certification schemes not included in the Union rolling work programme, as outlined in Articles 47 and 48 of the Act.

In view of its tasks, in particular its role in providing advice to ENISA and to the European Cybersecurity Certification Group and in issuing an opinion on the Union rolling work programme, the group does not qualify as a 'similar entity' in the sense of Article 2(2) of Commission Decision C(2016)3301 establishing horizontal rules on the creation and operation of Commission expert groups ('the horizontal rules')[2]. However, similar to an expert group/similar entity in the sense of the horizontal rules, the group is required to provide advice and assistance to the Commission, and this will constitute an important part of its work. Director General of Directorate-General Communications Networks, Content and Technology ('DG CNECT') will be applying by analogy the horizontal rules to the functioning of the group and the selection of its members.

3. Features of the Group

3.1. COMPOSITION

The group shall consist of up to 50 members.

In accordance with Article 22 and Recital 62 of the Act, the group shall be composed of:

'*members selected from among recognised experts representing the relevant stakeholders. In particular, it should be composed of members representing industry in balanced proportions, both on the demand side and the supply side of ICT products and ICT services, and including, in particular, SMEs, digital service providers, European and international standardisation bodies, national accreditation bodies, data protection supervisory authorities and conformity assessment bodies, and academia as well as consumer organisations'.*

[2] Commission Decision establishing horizontal rules on the creation and operation of Commission expert groups (C(2016) 3301 final).

In light of the aforementioned provisions of the Act and in compliance with the Commission's horizontal rules, members of the group shall be:

1. Organisations in the broad sense of the word, including in particular academic institutions, consumer organisations, conformity assessment bodies, standard developing organisations, companies and trade associations or other membership organisations active in Europe with an interest in cybersecurity certification.
   With a view to ensure a representation of a maximum number of stakeholders, priority will be given to trade associations or other membership organisations over single companies.
   Selection procedure: these organisations are the subject of this call.

2. The European Standardisation Organisations (CEN— European Committee for Standardisation, Cenelec— European Committee for Electrotechnical Standardisation, ETSI— European Telecommunications Standards Institute) and International Standardisation Bodies (International Organisation for Standardisation (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU))[3].
   Selection procedure: these organisations will be appointed directly by DG CNECT.

3. The European co-operation for Accreditation ('EA').
   Selection procedure: appointed directly by DG CNECT.

4. The European Data Protection Board (EDPB).
   Selection procedure: appointed directly by DG CNECT.

Organisations and public authorities shall nominate their representatives and shall be responsible for ensuring that their representatives provide a high level of expertise.

This person will be the permanent representative in the group. On an ad hoc basis, depending on the meeting agenda of the group, another representative can replace the permanent representative.

The Commission's Director General of Directorate-General Communications Networks, Content and Technology (DG CNECT) may refuse the nomination of a representative by an organisation if it considers this nomination inappropriate in light of the requirements specified in chapter 5 of this call. In such case, the organisation concerned shall be asked to appoint another representative.

3.2. APPOINTMENT

Members shall be appointed by DG CNECT from applicants complying with the requirements referred to in chapter 5 of this call.

[3] Regulation (EU) No 1025/2012 on European standardisation amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council

Members shall be appointed for three years. They shall remain in office until replaced or until the end of their term of office. Their term of office may be renewed.

In order to ensure continuity and the smooth functioning of the group, DG CNECT may establish a reserve list of up to 10 suitable candidates that may be used to appoint replacements. DG CNECT shall ask applicants for their consent before including their names on the reserve list[4].

Members who are no longer capable of contributing effectively to the group's deliberations, who in the opinion of DG CNECT 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 remainder of their term of office.

3.3. RULES OF ENGAGEMENT AND OPERATION OF THE GROUP

As provided for in Article 22 of the Act, the Stakeholder Cybersecurity Certification Group shall be co-chaired by representatives of DG CNECT and of ENISA, and its secretariat shall be provided by ENISA.

The group shall act at the request of DG CNECT in compliance with the Commission's horizontal rules on expert groups[5].

In principle, the group shall meet 3 times per year on Commission premises. In exceptional cases, the group may meet outside Commission premises.

DG CNECT shall ensure interaction with other DGs and other expert groups or engagement platforms, if necessary or relevant for the work of the expert group.

Members should be prepared to attend meetings systematically, to contribute actively to discussions in the group, to be involved in preparatory work ahead of meetings, to examine and provide comments on documents under discussion, and to act, as appropriate, as 'rapporteurs' on an ad hoc basis.

As a general rule, working documents will be drafted in English and meetings will be also conducted in English.

In principle, the group shall adopt its opinions, recommendations or reports by consensus. In the event of a vote, the outcome of the vote shall be decided by simple majority of the members. Members who have voted against or abstained shall have the right to have a document summarising the reasons for their position annexed to the opinions, recommendations or reports.

In agreement with DG CNECT, the group may by simple majority of its members decide that deliberations shall be public.

[4] See Article 10.9 of the horizontal rules (C(2016) 3301 final).
[5] See Article 13.1 of the horizontal rules (C(2016) 3301 final).

Participants in the activities of the group and sub-groups shall not be remunerated for the services they offer.

Travel expenses incurred by participants in the activities of the group and sub-groups shall be reimbursed by the Commission[6], upon their request.

Reimbursement shall be made in accordance with the provisions in force within the Commission and within the limits of the available appropriations allocated to the Commission departments under the annual procedure for the allocation of resources.

The members of the group and their representatives, 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 to the Commission's rules on security regarding the protection of Union classified information, laid down in Commission Decisions (EU, Euratom) 2015/443[7] and 2015/444[8]. Should they fail to respect these obligations, the Commission may take all appropriate measures.

On a proposal by and in agreement with DG CNECT, the Group shall adopt its rules of procedure on the basis of the standard rules of procedure for expert groups.

DG CNECT may invite experts with specific expertise on a subject matter on the agenda to take part in the work of the group or sub-groups on an ad hoc basis.

Individuals, organisations and public entities, such as EU bodies, offices or agencies and international organisations, may be granted an observer status, in compliance with the horizontal rules, by direct invitation[9]. 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. However, they shall not have voting rights and shall not participate in the formulation of recommendations or advice of the group.

DG CNECT may set up sub-groups for the purpose of examining specific questions on the basis of terms of reference defined by DG CNECT. Sub-groups shall operate in compliance with the horizontal rules and shall report to the group. They shall be dissolved as soon as their mandate is fulfilled.

3.4 TRANSPARENCY

Information about the work of the group shall be provided on a dedicated website.

As concerns the group composition, DG CNECT shall publish the following:

- the name of member organisations; the interest represented shall be disclosed.

[6] See Article 20 of the horizontal rules (C(2016) 3301 final).
[7] Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41).
[8] 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).
[9] See Article 16.1 of the horizontal rules (C(2016) 3301 final).

- the name of public entities.
- the names of observers.

DG CNECT shall make available all relevant documents, including the agendas, the minutes and the participants' submissions on the dedicated website. Access to it shall not be subject to user registration or any other restriction. In particular, DG CNECT shall ensure publication of the agenda and other relevant background documents in due time ahead of the meeting, followed by timely publication of minutes. Exceptions to publication shall only be foreseen where it is deemed that disclosure of a document would undermine the protection of a public or private interest as defined in Article 4 of Regulation (EC) No 1049/2001[10]. Personal data shall be collected, processed and published in accordance with Regulation (EU) 2018/1725.

4. Application procedure

Interested organisations are invited to submit their application to the European Commission, DG CNECT, following the instructions on the dedicated EUSurvey 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.

Organisations shall indicate the name of their proposed representatives in the group.

An application will be deemed admissible only if it is submitted by the deadline and includes the documents referred to below.

Supporting documents

Each application shall include:

- a CV of the representative proposed.

- a cover letter explaining the applicant's motivation for answering this call and stating what contribution the applicant could make to the group.

- a classification form duly filled in specifying the type of organisation, the interest represented and the policy area(s) (Annex I[11]).

- a selection criteria form duly filled in documenting how the applicant fulfils the selection criteria listed in chapter 5 of this call (Annex II[12]).

For individuals indicated by organisations as their representatives, a curriculum vitae (CV) shall also be provided, preferably not exceeding three pages. All CVs shall be submitted in the

[10] These 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.
[11] Available on EUSurvey
[12] Available on EUSurvey

European format (https://europass.cedefop.europa.eu/en/documents/curriculum-vitae/templates-instructions).

Deadline for application

The duly completed applications must be submitted by 12h00, on Tuesday, 17th September 2019 at the latest.

5. Selection criteria

DG CNECT will take the following criteria into account when assessing applications:

- competence (e.g. legal, economic, technical) and experience of the proposed representative 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.

- proven ability of the proposed representative to deliver strategic advice, including of scientific or technical nature, on issues relevant to cybersecurity certification, including in the above-mentioned areas of relevance for this call.

- other relevant competence, experience and hierarchical level of the proposed representative;

- representativeness of the organisation within a particular sector or group of stakeholders;

- contribution of the organisation to geographic balance of the group;

- good knowledge of English allowing the proposed candidate an active participation in the discussions.

6. Selection procedure

The selection procedure shall consist of an assessment of the applications performed by DG CNECT against the selection criteria listed in chapter 5 of this call, on the basis of a proposal by ENISA, followed by the establishment of a list of the most suitable applicants, and concluded by the appointment of the members of the group.

When defining the composition of the group, DG CNECT shall aim at ensuring, as far as possible, a high level of expertise, as well as a balanced representation of relevant know how and areas of interest and sectors, while taking into account the specific tasks of the group, the type of expertise required, as well as the relevance of the applications received.

In accordance with the Act, DG CNECT shall also ensure a balance between the different stakeholder groups as well as an appropriate geographical balance.

For any further information, please contact: CNECT-SCCG@ec.europa.eu