

Call for applications for the selection of members of the ECCC Strategic Advisory Group (SAG)

Contents

<u>Background</u>	2
<u>Scope of the Strategic Advisory Group</u>	3
<u>Tasks of the Strategic Advisory Group</u>	3
<u>Selection and appointment of the SAG members</u>	4
<u>Composition</u>	4
<u>Selection criteria</u>	5
<u>Eligibility criteria</u>	5
<u>Essential criteria – general and specific</u>	6
<u>Advantageous criteria</u>	8
<u>Application procedure and closing date</u>	8
<u>Selection Process</u>	9
<u>Protection of personal data</u>	10

Background

The European Cybersecurity Competence Centre (ECCC)¹ is a European Union (EU) body established by Regulation (EU) 2021/887² of the European Parliament and of the European Council.

The Regulation provides the ECCC with the mandate to support industrial technologies, research and innovation in the domain of cybersecurity, collaborating with the Network of National Coordination Centres (NCCs) and stakeholders from the Cybersecurity Competence Community (the Community). The ECCC manages EU financial resources dedicated to cybersecurity under the Digital Europe Programme (DEP)³ and the Horizon Europe Programme (HEP)⁴, and other EU programmes where appropriate, as well as additional contributions from Member States, to implement projects and initiatives on cybersecurity research, technology and industrial development.

The ECCC has adopted a Strategic Agenda⁵ for cybersecurity development and deployment, with a strong focus on supporting small and medium-sized enterprises (SMEs). Together with the Network of National Competence Centres (NCCs), it contributes to Europe's technological sovereignty and open strategic autonomy through joint investment in key cybersecurity projects.

The ECCC also promotes collaboration and knowledge-sharing among all relevant stakeholders, particularly members of the Cybersecurity Competence Community, as defined in Article 5 of the Regulation.

The Strategic Advisory Group supports this process by ensuring regular dialogue between the Competence Centre and the Community. It should represent stakeholders from the private sector, consumer organisations, academia, and other relevant actors, focusing on their priorities and bringing them to the attention of the Governing Board and the Executive Director.

Scope of the Strategic Advisory Group

In line with Article 18 of the ECCC Regulation, the SAG provides input to the activities of the Competence Centre including to the annual and multiannual work programmes. The SAG is composed of representatives of the private sector, consumers' organisations, academia and other relevant stakeholders. The Strategic Advisory Group should focus on issues relevant to stakeholders and bring them to the

¹ https://cybersecurity-centre.europa.eu/index_en.

² Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (OJ L 202, 8.6.2021, p. 1).

³ Digital Europe Programme established by Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240 (OJ L 166, 11.5.2021, p. 1).

⁴ Horizon Europe Programme established by Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013 (OJ L 170, 12.5.2021, p. 1).

⁵ Such Agenda is foreseen by the ECCC regulation. The ECCC Strategic Agenda, adopted by ECCC GB in March 2023 is available at: https://cybersecurity-centre.europa.eu/strategic-agenda_en

attention of the Governing Board and the Executive Director. The representation of the different stakeholders in the Strategic Advisory Group should be balanced, with particular attention paid to the representation of SMEs, to ensure that stakeholders are appropriately represented in the work of the Competence Centre.

Tasks of the Strategic Advisory Group

According to Article 20 of the ECCC regulation, the Strategic Advisory Group shall regularly advise the Competence Centre in respect of the performance of the Competence Centre's activities and shall ensure communication with the Community and other relevant stakeholders.

The Strategic Advisory Group shall also:

- (a) taking into account contributions from the Community and the working groups referred to in point (n) of Article 13(3) where relevant, provide and update on an ongoing basis strategic advice and input to the Executive Director and the Governing Board with regard to the Strategic Agenda, the annual work programme and the multiannual work programme within the deadlines set by the Governing Board;
- (b) advise the Governing Board on the establishment of working groups within the Community in accordance with point (n) of Article 13(3) on specific issues relevant to the work of the Competence Centre.
- (c) subject to approval by the Governing Board, decide on and organise public consultations open to all public and private stakeholders who have an interest in the area of cybersecurity, to collect input for the strategic advice referred to in point (a).

The Strategic Advisory Group shall meet at least three times a year. The meetings shall take place in Bucharest at the ECCC premises or other EU MS as required. The Strategic Advisory Group shall elect its Chair by a simple majority of its members.

Travel and subsistence expenses incurred in connection with the activities of the Group will be reimbursed by the ECCC.

Selection and appointment of the SAC members

The ECCC is opening a Call for Expression of Interest for Membership of the ECCC Strategic Advisory Group. The term of office of members of the Strategic Advisory Group is for two years, renewable once. The indicative starting date of the term is Q1/2026.

In accordance with the ECCC Regulation, the Governing Board shall appoint the **20 members** of the Strategic Advisory Group (SAG), acting on a proposal from the Executive Director from among the representatives of members of the Cybersecurity Competence Community (Community) mentioned in Article 8(2) of the Regulation other than representatives of Union institutions, bodies, offices and agencies.

Appointments for SAG members shall be made "*ad personam*". They shall therefore not delegate their responsibilities to another member, or to a third person and they shall not be representing, during the work for the SAG, their employer or any particular interests.

It should be noted that representatives of the Commission and of other Union institutions, bodies, offices and agencies, in particular ENISA, cannot be part of the 20 SAG members, however they may be invited by the Strategic Advisory Group to participate in and support its work.

Composition

In the composition of the Strategic Advisory Group, the Governing Board shall strive to achieve a balanced representation of the Community between **scientific, industrial and civil society entities, demand and supply-side industries, large enterprises and SMEs**, as well as balanced representation in terms of geographical provenance and gender. It shall also aim to achieve an **intra sectorial balance**, having regard to the cohesion of the Union and all the Member States in the area of **cybersecurity research, industry and technology**.

To ensure compliance with these requirements, the Strategic Advisory Group shall be composed of members coming from entities that are registered in the Community and should include:

- (a) At least 3 members representing scientific/research/academic community.
- (b) At least 3 members representing industry, demand and supply-side industries, large enterprises, including SMEs, stakeholders in sectors that have an interest in cybersecurity and that face cybersecurity challenges.
- (c) At least 3 members representing public entities and other entities dealing with cybersecurity operational and technical matters.
- (d) At least 3 members representing different sectors of high criticality as identified in Annex I of the NIS 2 Directive 2555/2022.

Selection criteria

Eligibility criteria

To be eligible, a candidate must:

- Be citizen of an EU or EEA country.
- Work for an entity which is eligible to be registered in the Community, as defined in Article 8 of regulation 887/2021⁶ of the ECCC. *(At the application stage, the candidate shall only confirm that their company is eligible to be included in the Community. At the final appointment, the criteria must be confirmed)*
- Possess: (a) a level of education which corresponds to completed university studies, attested by a diploma, where the normal period of university education is four years or more; or (b) a level of education which corresponds to completed university studies, attested by a diploma, and appropriate professional experience of at least one year, where the normal period of university education is at least three years (this one year's professional experience cannot be included in the postgraduate professional experience required below).
- Have at least 10 years of professional experience in one or more cybersecurity domains, such as research, industrial development, offering, implementing, or deploying professional services or products including training and education on information security.
- Have an excellent command of English.

Candidates will not be eligible if:

- They have been convicted, by final judgment, of an offence related to their professional conduct.
- They have been convicted, by final judgment, of fraud, corruption, participation in a criminal organisation, or any other illegal activity harmful to the EU's financial interests.

Essential criteria – general and specific

To ensure a balanced representation of stakeholders as indicated in the Regulation, candidates shall comply with the following general criteria and with specific criteria depending on the specific domain that they will represent:

⁶ Only representatives of entities which are not controlled by a third country or by an entity established in a third country shall be eligible; The candidate should also have the agreement of his/her employer for taking up the role for SAC. Please note that staff of EU institutions, bodies, offices and agencies **are not eligible**.

General criteria

- Good knowledge of EU cybersecurity policies, regulations, and awareness of global cybersecurity challenges
- Strong communication skills and ability to represent stakeholders' perspectives
- Experience working with expert networks or professional organisations
- Ability to draft policy documents and technical or scientific reports
- At least 3 years of proven expertise (acquired in the last 10 years) in areas relevant to the ECCC Strategic Agenda⁷ and Work Programme 2025-2027 as available on the ECCC website.
- Expertise in non-technical dimensions of cybersecurity – including legal, strategic, governance, social or educational aspects are also welcomed.

Specific criteria

- (a) For the candidates representing scientific/research/academic community
 - Broad knowledge of cybersecurity research domain and high-level expertise for at least one specific area/domain/sector of interest for ECCC relevant for the call.
 - At least 5 years' experience of working in academia/research/scientific community with a research and/or educational role that is relevant to the call.
 - Experience of representing an academia/scientific organisation on a national, European or international committee or advisory boards.
 - List of publications with at least 3 articles published in the last 5 years in at least one of the topics of interest for the ECCC (see above)
- (b) For the candidates representing **industry**, demand and supply-side industries, large enterprises, **including SMEs**, stakeholders in sectors that have an interest in cybersecurity and that face cybersecurity challenges

- Broad knowledge of cybersecurity domain and for the specific domain challenges for demand and supply-side industries, large enterprises, including SMEs, stakeholders including sectors of NIS 2 Directive.
 - At least 5 years' experience of working in industry, demand and supply-side industries, large enterprises, including SMEs, stakeholders in sectors that have an interest in cybersecurity and that face cybersecurity challenges.
 - Experience of representing the industry/SMEs community in national or international committee or advisory boards.
 - Been actively involved in the industry/SMEs Community with publications, conferences, keynote, presentations or contributions to national reports or strategic documents.
- (c) For the candidates representing **public entities** and other entities dealing with cybersecurity operational and technical matters.
 - Broad knowledge of cybersecurity domain and challenges of public sector, including cybersecurity challenges for the sectors of NIS 2 Directive.
 - At least 5 years' experience of working in public entities and other entities dealing with cybersecurity operational, and technical matters or non-technical but equally crucial dimensions of cybersecurity – including legal, strategic, governance, social or educational aspects.
 - Experience of representing a public sector entity on a national, European or international committee or advisory board.
 - Been actively involved in the Community with publications, conferences, keynote, presentations or contributions to national reports or strategic documents.

Advantageous criteria

- Cross-sector or cross-domain expertise, covering multiple technology areas or sectors, including legal, strategic, governance, or social aspects.
- Previous participation in EU task forces or committees providing consultations on topics relevant to this call.
- Experience collaborating with international organizations, or professional exposure and activities beyond the EU.

Each criterion will be evaluated, and candidates will be awarded points according to their alignment with the above criteria

Application procedure and closing date

The application shall include:

- A completed application form including the Curriculum Vitae in the Europass format⁸ The application shall be completed online at the following link <https://ec.europa.eu/eusurvey/runner/SAGApplicationForm>

Applications should be submitted not later than **30 December 2025**, 23:59 Bucharest time zone.

Incomplete applications or applications received after the deadline will not be considered. Only the applications filled in at the link specified above, within the deadline will be taken into consideration. Please note that filling in the form will take time as you need to provide detailed examples of your expertise, to fill in a motivation letter of maximum 5000 characters and to attach your CV in the Europass format. The relevance of the examples you provide will support your selection.

Selection Process

This Call is for the selection of up to twenty (20) Strategic Advisory Group members.

Upon receipt of the applications, the ECCC will perform an eligibility check and preliminary assessment on all applications received and will draw up a preliminary list with the candidates fulfilling all the eligibility requirements.

The preliminary list of candidates will be forwarded to a Selection Committee, composed of:

1 ECCC staff member who will chair the panel

1 representative of the ECCC Governing Board

1 representative of the NCC Network

1 representative of the European Commission

⁸ <http://europass.cedefop.europa.eu/en/documents/curriculum-vitae/templates-instructions>

Secretariat support will be provided by the HR team of the ECCC.

After receiving the preliminary list of candidates from the ECCC, the Selection Committee will assess the applications received in accordance with all the criteria laid down in this call for expression of interest and will draft a shortlist with the candidates with the highest scores.

The composition of the shortlist shall ensure a balanced representation of the Community in terms of the areas of expertise, gender and geographical distribution. During this phase the panel may decide, if they consider it necessary, to conduct online interviews with applicants.

From this shortlist, the ECCC Executive Director will draw a final list with the 20 most qualified candidates to be presented to the Governing Board for approval, ensuring the balance on the composition as described above.

This shortlist prepared by the Selection Committee will be retained and used, if needed, during entire mandate of the SAG for further appointments/replacements.

Protection of personal data

Personal data shall be collected, processed and published in accordance with Regulation (EU) 2018/1725. For further information, please refer to the data protection notice available on the application form.