Call for Expressions of Interest

ENISA M-CEI-21-T41

“Establishment of a List of Individual External Experts to Assist ENISA”

TECHNICAL DESCRIPTION

CONTENTS

TECHNICAL DESCRIPTION

1. INTRODUCTION

With the Cybersecurity Act (Regulation (EU) No 881/2019), which was enacted in June 2019, the European Union Agency for Cybersecurity (ENISA) became a key instrument for realising the EU's ambition of significantly reinforcing cybersecurity across Europe.

ENISA's mission is to achieve a high common level of cybersecurity across the Union in cooperation with the wider community. It does this through acting as a centre of expertise on cybersecurity, collecting and providing independent, high quality technical advice and assistance to Member States and EU bodies on cybersecurity. It contributes to developing and implementing the Union's cyber policies. ENISA's aim is to strengthen trust in the connected economy, boost resilience and trust of the Union's infrastructure and services and keep our society and citizens digitally secure.

As overarching objectives, ENISA should:

1. be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks.

2. assist the Union institutions, bodies, offices and agencies, as well as Member States, in developing and implementing Union policies related to cybersecurity, including sectoral policies on cybersecurity.

3. support capacity-building and preparedness across the Union by assisting the Union institutions, bodies, offices and agencies, as well as Member States and public and private stakeholders, to increase the protection of their network and information systems, to develop and improve cyber resilience and response capacities, and to develop skills and competencies in the field of cybersecurity.

4. promote cooperation, including information sharing and coordination at Union level, among Member States, Union institutions, bodies, offices and agencies, and relevant private and public stakeholders on matters related to cybersecurity.

5. contribute to increasing cybersecurity capabilities at Union level in order to support the actions of Member States in preventing and responding to cyber threats, in particular in the event of cross-border incidents.

6. promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation, with a view to increasing the transparency of the cybersecurity of ICT products, ICT services and ICT processes, thereby strengthening trust in the digital internal market and its competitiveness.

7. promote a high level of cybersecurity awareness, including cyber-hygiene and cyber-literacy among citizens, organisations and businesses.

In order to contribute to the achievement of these ambitious objectives, ENISA details its planned activities in the Single Programming Document, which encompasses the Annual and Multi-Annual Work Programmes. This document, which is published on an annual basis, is available on ENISA's website: http://www.enisa.europa.eu/publications/programmes-reports

2. TASKS AND ACTIVITIES OF THE EXPERTS

The subject matter experts could be expected to perform one or more of the following tasks:

- Provide specific contributions according to their expertise in the area of expertise selected.
- Be appointed as members or coordinators of expert working groups set up to work on specific projects. The actual size of exert working groups is determined in line with operational priorities.
- Carry out duties remotely as no work facilities are made available by ENISA.
- Participate in any face-to-face meetings and teleconferences organised.

It should be noted that the subject matter experts are appointed "ad personam" and will not be considered as representatives of their organization or affiliation they are employed with.

For this reason, the successful applicant will be required to complete a 'Legal Entity' identification form (LE) in their own name, as a 'natural person' and not in the name of their employer. If the applicant has a 100% owned private company, then this may exceptionally be used to complete the LE form.

3. FIELDS OF EXPERTISE SOUGHT

In implementing its yearly work programme, ENISA will from time to time need to involve external subject matter experts to participate in and provide their expertise for various projects within the below-mentioned Strategic Objectives; the range of activities is determined in line with the annual work program of the Agency as documented in the Single Programming Document. Expert participation in ENISA projects is a manifestation of stakeholder's involvement and ability to mobilise expertise not just from within the Agency but also from among (high) level individual Experts in the market. From time to time, these Experts may work alongside representatives or experts of EU Member States who may also contribute to the same project.

To this effect, ENISA hereby seeks to establish a list from which suitably qualified persons will be selected to assist the Agency in carrying out various work activities foreseen in its Strategic Objectives. It is emphasised that not all activities will need assistance from external subject matter experts.

ENISA welcomes applications from experts in diverse sectors such as: academia, research, industry, EU institutions, International Organisations etc.

Based on the Cybersecurity Act (CSA), ENISA has established seven (7) Strategic Objectives facilitating the implementation of ENISA's mandate, which are described below:

SO1 - Strategic Objective:

“Empowered and engaged communities across the cybersecurity ecosystem”

Context: Cybersecurity is a shared responsibility. Europe strives for a cross-sectoral, all-inclusive cooperation framework. ENISA plays a key role in stimulating active cooperation between the cybersecurity stakeholders in Member States and the EU institutions and agencies. It strives to ensure complementarity of common efforts, by adding value to the stakeholders, exploring synergies and effectively using limited cybersecurity expertise and resources. Communities should be empowered to scale up the cybersecurity model.

What we want to achieve:

- An EU-wide, state of the art body of knowledge on cybersecurity concepts and practices, that builds cooperation amongst key actors in cybersecurity, promotes lessons learned, EU expertise and creates new synergies.
- An empowered cyber ecosystem encompassing Member States authorities, EU institutions, agencies and bodies, associations, research centres and universities, industry, private actors and citizens, who all play their role in making Europe cyber secure;

Fields of expertise:

1.1 - Stakeholder strategy and management	*1.2 - Cybersecurity activities in education and / or cybersecurity skills development*
1.3 - EU Cybersecurity Blueprint	*1.4 - Awareness raising campaigns development in cybersecurity (sectors, industries, capacities)*
1.5 - Cyber hygiene and cyber literacy	*1.6 – Cybersecurity research and innovation*

SO2 - Strategic Objective:

“Cybersecurity as an integral part of EU policies”

Context: Cybersecurity is the cornerstone of digital transformation and the need for it permeates all sectors, therefore it needs to be considered across a broad range of policy fields and initiatives. Cybersecurity must not be restricted to a specialist community of technical cyber experts. Cybersecurity must therefore be embedded across all domains of EU policy. Avoiding fragmentation and the need for a coherent approach while taking into account the specificities of each sector is essential.

What we want to achieve:

- Proactive advice and support to all relevant EU-level actors bringing in the cybersecurity dimension in policy development lifecycle through viable and targeted technical guidelines;
- Cybersecurity risk management frameworks that are in place across all sectors and followed throughout the cybersecurity policy lifecycle.

Fields of expertise:

2.1 - Current cybersecurity policy frameworks, (e.g. NISD, eIDAS, ePrivacy, EECC, 5G)	*2.2 - New cybersecurity policies in response to emerging technological, societal and economic trends, (e.g. AI, Digital Wallets, Once Only Principle)*
2.3 - Policy analysis /recommendations /guidelines /promotion of existing or emerging policies	*2.4 - Policy research*

SO3 - Strategic Objective:

“Effective cooperation amongst operational actors within the Union in case of massive cyber incidents”

Context: The benefits of the European digital economy and society can only be fully attained under the premise of cybersecurity. Cyber-attacks know no borders. All layers of society can be impacted and the Union needs to be ready to respond to massive (large scale and cross-border) cyber-attacks and cyber crisis. Cross-border interdependencies have highlighted the need for effective cooperation between Member States and the EU institutions for faster response and proper coordination of efforts at all levels (strategic, operational, technical and communications).

What we want to achieve:

- Continuous cross-border and cross layer support to cooperation between Member States as well as with EU institutions. In particular in view of potential large scale incidents and crises, support the scaling up of technical operational, political and strategic cooperation amongst key operational actors to enable timely response, information sharing, situational awareness and crises communication across the Union;

- Comprehensive and rapid technical handling upon request of the Member States to facilitate technical and operational needs in incident and crises management.

Fields of expertise:

3.1 - Cybersecurity incident / event life cycle (incident reporting, triage, resolving, analysis, recovery)	*3.2 - Vulnerability life cycle (responsible disclosure, vulnerability management)*
3.3 - Cybersecurity crises management, (including maturity and evaluation frameworks)	*3.4 - Management of incident response (Procedures; Processes; Organization, management and operations of team; maturity and evaluation frameworks)*
3.5 - DevSecOps and development/use of tools	*3.6 - Asset management*
3.7 - Cyber threat Intelligence / Threat hunting / Situational awareness	*3.8 - Cooperation (international cooperation, community support, cooperation with Law Enforcement Agencies and other stakeholders)*
3.9 - Handling of classified information	

SO4 - Strategic Objective:

“Cutting-edge competences and capabilities in cybersecurity across the Union”

Context: The frequency and sophistication of cyberattacks is rising speedily, while at the same time the use of ICT infrastructures and technologies by individuals, organisations, and industries is increasing rapidly. The needs for cybersecurity knowledge and competences exceeds the supply. The EU has to invest in building competences and talents in cybersecurity at all levels, from the non-expert to the highly skilled professional. The investments should focus not only on increasing the cybersecurity skillset in the Member States but also on making sure that the different operational communities possess the appropriate capacity to deal with the cyber threat landscape.

What we want to achieve:

- Aligned cybersecurity competencies, professional experience and education structures to meet the constantly increasing needs for cybersecurity knowledge and competences in the EU;
- An Elevated base-level of cybersecurity awareness and competences across the EU while mainstreaming cyber into new disciplines;
- Well prepared and tested capabilities with the appropriate capacity to deal with the evolving threat environment across the EU.

Fields of expertise:

4.1 - Designing / Developing training	*4.2 - Delivering / Organising / Evaluating training*
4.3 - Training the trainers	*4.4 - Design / Implement a cyber range*
4.5 - Risk management methodologies	*4.6 - Risk assessment practices*
4.7 - Cybersecurity training and exercises	*4.8 - Information sharing models and techniques*
4.9 - Competence mapping	*4.10 - Cybersecurity strategies*

SO5 - Strategic Objective:

“High level of trust in secure digital solutions”

Context: Digital products and services bring benefits as well as risks, and these risks must be identified and mitigated. In the process of evaluating security of digital solutions and ensuring their trustworthiness, it is essential to adopt a common approach, with the goal to strike a balance between societal, market, economic and cybersecurity needs. A neutral entity acting in a transparent manner will increase customer trust on digital solutions and the wider digital environment.

What we want to achieve:

- Cyber secure digital environment across the EU, where citizens can trust ICT products, services and processes through the deployment of certification schemes in key technological areas;

Fields of expertise:

5.1 - ICT cybersecurity standardisation	*5.2 - ICT product, service or process security certification*
5.3 - Technical specifications for products, services, processes	*5.4 - Risk assessment and/or assurance level definition experience*
5.5 - Establishment, monitoring, maintenance, , review of certification schemes	*5.6 - Security audit and/or audit methodology of information systems*
5.7 - Security evaluation, conformity assessment, evaluation methodology of ICT products, services and processes	*5.8 - Penetration testing of ICT products and / or of information systems (including vulnerability assessment and handling)*
5.9 - Secure development lifecycle	*5.10 - Risk management / assessments in relation to cybersecurity certification*
5.11 - Evaluation of cybersecurity testing and conformity assessment facilities	*5.12 - Strategic cybersecurity market analysis*
5.13 - Applied research and innovation in trusted solutions	*5.14 Secure labelling of product, services and processes*
5.15 Good practices in market, certification and standardisation	*5.16 Vulnerabilities management of certified products services and processes*
5.17 European and international standardisation governance	*5.18 European and international research agenda*

SO6 - Strategic Objective:

"Foresight on emerging and future cybersecurity challenges"

Context: Numerous new technologies, still in their infancy or close to mainstream adoption, would benefit from the use of foresight methods. Through a structured process enabling dialogue among stakeholders, decision- and policy-makers would be able to define early mitigation strategies that improve the EU resilience to cybersecurity threats and find solutions to address emerging challenges.

What we want to achieve:

- Understanding emerging trends and patterns using foresight and future scenarios that contribute to mitigating our stakeholder's cyber challenges;

- Early assessment of challenges and risks from the adoption of and adaptation to the emerging future options, while collaborating with stakeholders on appropriate mitigation strategies.

Fields of expertise:

6.1 - National and / or EU Cybersecurity Research	*6.2 - Forecasting and future studies*
6.3 - Horizon scanning	*6.4 - Scenario planning*
6.5 - Strategic or corporate foresight	*6.6 - Foresight methods (e.g. Delphi analysis, simulation/gaming, trend analysis / extrapolation)*
6.7 - Technology forecasting	*6.8 - Transition from research into development and innovation*
6.9 - Prediction markets	*6.10 - Identification of future research and innovation needs and priorities*
6.11 - Identification of future challenges and opportunities in cybersecurity research	*6.12 - EU research funding programmes*

SO7 - Strategic Objective:

“Efficient and effective cybersecurity information and knowledge management for Europe”

Context: The energy that fuels the mill of cybersecurity is information and knowledge. For cybersecurity professionals to be efficient at tackling our objectives, to work in a constantly moving environment – in terms of digital developments as well as with regard to actors – to face the challenges of our time, we need a continuous process of collecting, organising, summarising, analysing, communicating, and maintaining cybersecurity information and knowledge. All phases are essential to ensure that information and knowledge is shared and expanded within the EU cybersecurity ecosystem.

What we want to achieve:

- Shared information and knowledge management for the EU cybersecurity ecosystem in an accessible, customised, timely and applicable form, with appropriate methodology, infrastructures and tools, coupled and quality assurance methods to achieve continuous improvement of services.

Fields of expertise:

7.1 - Threat landscapes	*7.2 - Emerging technologies (Internet of Things, artificial intelligence, 5G, distributed ledgers, etc.)*
7.3 - Cryptology	*7.4 - Quantification of cybersecurity (metrics, assessment, impact analysis)*
7.5 - Cybersecurity rankings, indexes, trend analysis	*7.6 - Cybersecurity incident reporting*
7.7 - Cybersecurity knowledge management	

4. LIST OF SECTORS

Applicants can further define their interest in ‘Fields of expertise’ on the Application form, by selecting which ‘Sector’ their experience relates to.

Here are the sectors available on the application form (in alphabetical order):

5G	European Electronic Communications Code
Artificial Intelligence	Finance / Banking
Aviation	GDPR
Big data	Governmental/EU-I
Civil protection	Healthcare
Cloud computing	ICT security policies, specifications and best practices
Common Criteria	Incident notification/reporting
Connected devices	Incident response teams (CSIRTs, SOCs, PSIRTs)
Critical infrastructure	Information sharing
Cryptography	Insurance
CSA	Internet infrastructure
Cybersecurity - compliance aspects	Internet of Things - consumers
Cybersecurity - consumer	Law enforcement
Cybersecurity - economics	Maritime
Cybersecurity - industrial systems	NISD 1
Cybersecurity - public sector	NISD 2
Cybersecurity for SMEs	NISD sectorial regulations
Cybersecurity market analysis / quantitative and qualitative methods	Once Only
Cybersecurity of ICT enabled machinery	PKI
Defence	PSD2
Digital identity management	Radio equipment
Digital Infrastructures	Rail
DORA	Research and development
eIDAS	Secure software development
Electricity CODE	Security of supply chain
Electronic communications	Societal/psychological, behavioral aspects of cybersecurity
Energy	Trust services
ePrivacy	Vulnerability disclosure
European Critical Infrastructures Directive	Water

5. ELIGIBILITY CRITERIA

Based on the self-declared application forms received, only candidates who meet the following minimum criteria will automatically be considered to be included in the list of external experts dependent on endorsement by an evaluation committee:

- Have fully completed their application form;
- Are a national of, or working for a legal entity of one of the Member States of the EU or EEA;
- Have a bank account in an EU Member State or EEA;
- Have proven experience in using English as a working language;
- Have minimum **3 years of experience** in the selected areas and fields of expertise;
- Have minimum **12 months of experience** in the selected areas and fields of expertise **during the last 5 years**;
- A **motivation letter** (500 words maximum), which establishes your incentive to be accepted as an expert for ENISA, as well as the capability of the applicant to work with others in a multicultural environment;
- CV preferably in Europass[1] format.

The evaluation committee may exceptionally further consider candidates who are close to the minimum requirements for years of experience or who have a unique skillset, for inclusion in the List.

6. SELECTION CRITERIA

Applicants will be evaluated according to their technical and professional capacity to meet the requirements of the Field(s) for which they are applying, following the criteria below:

- Relevance of their current job responsibilities and expertise to each of the 'Fields' applying for.
- Professional certifications held and publications will be taken into consideration.
- Their experience based on previous participation in similar projects; in particular, participation in relevant EU projects will be considered an advantage.

More specifically, an applicant should provide the following documentation/information:

- A **list of projects or publications** related to their declared field(s) of interest in the past 3 years. Without evidence of recent activity then it will be difficult to judge the applicant's suitability and level of experience.
- **Professional certifications** (e.g. CISSP, CISA etc.) and references (e.g. links) to **publications**.

[1] https://europass.cedefop.europa.eu

7. DURATION OF THE LIST OF EXPERTS

The CEI List of Experts compiled as a result of this procedure will be valid for a period of up to 5 years. The CEI will remain open to new applications for this whole period until 3 months before the end of the 5th year. New applications will be evaluated on a regular basis in order to update the List with successful applicants.

8. ESTIMATED BUDGET

It is anticipated that a budget of up to (approx.) €1.300.000 can be made available per year for the various projects covered by this CEI. Each selected Expert will be remunerated with a **fixed fee of €450 per person-day** plus any travel and subsistence related costs, which will be based on ENISA's applicable rules.

A successful applicant who is added to the CEI List may be invited to participate in one or more projects, but only up to a maximum of **€15.000** per calendar year. This is fully in accordance with EU procurement rules, which state that a maximum amount of **€15.000** (including costs) can be paid to any individual expert **by direct award** during the course of one calendar year.

8. DATA PROTECTION

All Data will be processed in accordance with Regulation (EU) 2018/1725 ('the EDPR'). The Data Protection notice for ENISA CEI External Experts can be found via this link:
https://www.enisa.europa.eu/procurement/related/data-protection-notice-for-enisa-cei-external-experts.pdf

9. GENERAL

It is clarified that the Agency is not limited to only appointing experts registered in this database. It may select in a transparent manner any individual expert with the appropriate skills not included in the database, if deemed appropriate and in duly justified cases.

Please note that for any particular project, the Agency has the possibility under the regulations governing Calls for Expressions of Interest to conduct a simplified tender procedure whereby all Experts already placed on the List of Experts for a particular field, will be invited to provide a tailored offer for the project. The offers received will then be evaluated on the basis of relevance and experience for the specific project, with the best submission evaluated being awarded the contract.

It is also noted that applicants that do not wish to or cannot be remunerated due to their primary employment contracts, are also eligible to apply for inclusion in the List of Experts, indicating this in the respective field of the CEI Application form. These applicants will still be entitled to reimbursement of any travel and subsistence costs incurred from their participation in a project, should they wish to be reimbursed.

Your completed 'Application form', together with all other relevant documentation supporting your application, must be sent only via email to cei-applications@enisa.europa.eu.