Call for Expressions of Interest

ENISA M/CEI/17/T01

"Experts for assisting in the implementation of the annual ENISA Work Programme"

TECHNICAL DESCRIPTION

(2018 Update)

CONTENTS

TECHNICAL DESCRIPTION

1. INTRODUCTION

The emergence of cyber security as a subject in its own right, where the goals and objectives are linked to global considerations and the emphasis is on international collaboration, represents a fundamental change in the way in which information security is evolving. The core mission of ENISA – to foster the development of a strong culture of NIS throughout the EU is perfectly aligned with this development and the recently adopted NIS Directive. The Agency is well positioned to assist the Commission and the Member States in defining and implementing effective strategies for dealing with cyber threats throughout the next decade.

The main tasks of ENISA based on its Regulation (EU) No 526/2013 aim to (a) support the development of Union network and information security policy and law, (b) support Member States in their efforts to develop and improve the prevention, detection and analysis of and the capability to respond to network and information security problems and incidents, (c) support the organisation and running of Union network and information security exercises, (d) promote cooperation between national and governmental CERTs or Computer Security Incident Response Teams (CSIRTs), and (e) support research and development and standardisation for risk management and for the security of electronic products, networks and services. Based on the above ENISA core activities span in the areas of threat/risk assessment, Critical Information Infrastructure Protection (CIIP), support of operational communities such as the CSIRT community, policy implementation (e.g. National cyber security strategies), standardisation and privacy and data protection.

The Agency has put a considerable amount of effort into improving the way it interacts with its different stakeholder communities and ensuring that stakeholder requirements are well understood and reflected by the work programme. Whilst the core areas have not changed, the approach of delivering services has changed significantly. The Agency has developed from an ‘activities-based’ approach, through a ‘deliverables-based’ approach to what could now be best described as an impact driven approach.

The yearly ENISA work programmes result from a consultation process involving both the ENISA Permanent Stakeholder Group (PSG) and the Management Board (MB). This process has enabled the Agency to increase its focus on areas that are both strongly aligned with the European policy agenda and also considered as core areas of competency for the Agency. The Yearly Work Programmes of ENISA can be found on the ENISA website: http://www.enisa.europa.eu/publications/programmes-reports

Please see the table below which provides an indicative summary of the 2018 Activities and related Objectives for ENISA: (this Annex will be updated as required in future years).

2. ACTIVITIES

***Activity 1 - Expertise*.** **Anticipate and support Europe in facing emerging network and information security challenges**
Objective 1.1. Improving the expertise related to Network and Information security
Objective 1.2. NIS Threat Landscape and Analysis
Objective 1.3. Research & Development, Innovation
Objective 1.4. Response to Article 14 Requests under Expertise Activity
Activity 2 - Policy. **Promote network and information security as an EU policy priority**
Objective 2.1. Supporting EU policy development.
Objective 2.2 Supporting EU policy implementation
Objective 2.3. Response to Article 14 Requests under Policy Activity
Activity 3 - Capacity. **Support Europe maintaining state-of-the-art network and information security capacities**
Objective 3.1. Assist Member States' capacity building.
Objective 3.2. Support EU institutions' capacity building.
Objective 3.3. Assist in improving general awareness
Objective 3.4. Response to Article 14 Requests under Capacity Activity
***Activity 4 - Community*.** **Foster the emerging European network and information security community**
Objective 4.1. Cyber crisis cooperation
Objective 4.2. CSIRT and other NIS community building.
Objective 4.3 Response to Article 14 Requests under Community Activity

The Activities for 2018 are further detailed:

Activity 1 - Expertise.

‘Anticipate and support Europe in facing emerging network and information security challenges’

This activity aims at developing and maintaining a high level of expertise of EU actors taking into account evolutions in NIS. It covers:

- the baseline security requirements, more specifically, minimum security requirements for Operators of Essential Services (OES, as they are referred in NIS Directive but especially for energy, health, finance and transportation) and recommendations for security measures on IoT (Internet of Things) field.
- the threat landscape
- activities related to research, development and innovation.

Activity 2 - Policy.

'Promote network and information security as an EU policy priority'

In this activity ENISA supports EU policy development and EU policy implementation in the areas of security and privacy. More specifically, this area includes supporting:

- the vision towards a Digital Single Market for high quality NIS products and services
- Technical implementation of EU policies and regulatory acts, such as eIDAS, GDPR, EU Telecommunications framework, ePrivacy Directive etc.
- Implementation of the NIS Directive. This means contribution to the cooperation group and especially to the development of good practices for identification of OES (criteria) and development of guidelines for the implementation of Mandatory Incident Reporting.

Activity 3 - Capacity.

'Support Europe maintaining state-of-the-art network and information security capacities'

Under this activity, ENISA develops actions related to the operational security capacity-support programme. More specifically, these actions include:

- updating and provision of trainings as well as guidelines for strengthening the national and governmental CSIRTs capabilities of EU Member States.
- assisting EU Member States to develop and assess their capabilities in the area of National Cyber Security Strategies (NCSS)
- assisting private sector capacity building in areas such as cyber insurance

Activity 4 - Community.

'Foster the emerging European network and information security community'

ENISA continues to support the cooperation among CSIRTs, within an EU Member States CSIRTs network. As it is provisioned by the NIS Directive, ENISA provides the secretariat of the network of CSIRTs and supports this cooperation by developing and providing guidance and good practices in the area of operational community efforts, such as on information exchange. Moreover, ENISA continues to support the fight against cybercrime and the collaboration between CSIRTS and law enforcement.

3. AREAS OF EXPERTISE SOUGHT

In implementing its yearly work programme, and in the context of its efforts towards engaging external stakeholders in its work as much as possible, ENISA would also like to involve external subject matter experts to participate in specific projects and provide their expertise for various projects within the above mentioned Activities.

To this effect, ENISA hereby seeks to establish a list from which NIS experts will be selected to assist the Agency in carrying out various work activities foreseen in its Activities and related Outputs. It is emphasised that not all activities and outputs will need assistance from external subject matter experts.

ENISA welcomes applications from experts in many sectors, i.e. academia, research, industry, EU institutions, International Organisations etc. Also, in terms of expertise sought, this would depend

on the projects for which assistance is required; in general, ENISA would need assistance in the following 'Fields' of expertise:

A. Technical expertise in ICTs and emerging application areas *(including but not limited to the following):*
1) Internet of Things, eHealth, cyber insurance, smart infrastructures, Smart Grids, Mobile technologies, network interdependencies, ICS-SCADA, RFID, etc. 2) Data Protection and Privacy (including privacy enhancing technologies, privacy impact assessment, security measures for data protection, privacy seals and personal data breaches) 3) Electronic Identification and Trust Services (including interoperability and security of electronic identification schemes, electronic ID cards, electronic authentication, digital signatures, website authentication, security and auditing schemes for Trust Service Providers, etc.) 4) Statistical analysis in this field of activity
B. ICT Security Standardisation and certification *(including but not limited to the following):*
1) Applied cryptography (algorithms, protocols, standards) 2) Information security risk management: expertise and experience in conducting risk assessment and risk management exercises, using appropriate risk management methodologies and tools - Risk and threat analysis 3) Security awareness / Advocacy campaign 4) Resilience of communication networks 5) Existing products and services certification schemes in the areas of security and privacy 6) Statistical analysis in this field of activity
C. Technical expertise in Critical Information Infrastructure Protection (CIIP) and CSIRTs Cooperation *(including but not limited to the following):*
1) Cyber exercises: Support and Incident development and national contingency plans 2) Cyber crisis management 3) Incident response and handling, CSIRT cooperation and law enforcement cooperation etc. 4) Incident Reporting for 'article 13a' of the Telecom Framework Directive and 'article 19' of the eIDAS Regulation 5) Security measures according to International standards, best practices and incident reporting requirements for CIIP Areas (energy, transport, health, digital infrastructure, finance and banking sector, drinking water supply and distribution,) 6) Statistical analysis in this field of activity
D. Legal expertise in NIS *(including but not limited to the following):*
1) Policy monitoring activity 2) Analysis of the legal framework relevant for information sharing, e.g., among CSIRTs and between CSIRTs and law enforcement agencies 3) Digital forensics 4) Providing assistance to MS for the implementation of NIS Directive 5) EU legal framework on data protection and privacy 6) Identification criteria of OES and building cyber security capabilities 7) Statistical analysis in this field of activity
E. NIS aspects of cybercrime *(including but not limited to the following):*
1) CSIRT and law enforcement cooperation, 2) Operational cooperation and information exchange in the CSIRT network 3) Statistical analysis in this field of activity

4. TASKS AND ACTIVITIES OF THE NIS EXPERTS

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

- Provide specific contributions (written and oral) according to their expertise in the project selected.
- Be appointed as members or coordinators of expert working groups set up to work on specific projects. Normally these groups consist of 10 - 15 experts.
- Participate in any face-to-face meetings and teleconferences organised.
- Act as ambassadors for ENISA activities (e.g. disseminate the results to their affiliations and organisations, report in various events/presentations, etc.).

It should be noted that the NIS experts are appointed "ad personam" and will not be considered as representatives of their affiliation or organization 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% private family company, then this may also be used to complete the LE form.

5. 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 one or more of the 'Fields' outlined above.
- Professional certifications they may hold and publications will be taken into consideration.
- Their experience based on their previous participation in similar projects; in particular, participation in relevant EU projects will be considered an advantage.
- English as a working language

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

- A **Curriculum Vitae**, preferably in the EU format; the template (preferably in English) can be downloaded from the following web link: https://europass.cedefop.europa.eu
- A **list of projects or publications** related to their declared fields of interest in the past 3 years. Without evidence of recent activity then it will be difficult for the evaluation committee to judge the applicant's suitability and level of experience.
- **Professional certifications** (e.g. CISSP, CISA etc.) and references (e.g. links) to **publications**.
- **Self-assessment of his/her expertise** in the fields (sub-fields) indicated in the table on page 6.
- Information on **languages** in which the applicant is proficient should also be indicated on the application form.

6. DURATION OF THE LIST of NIS EXPERTS

The official CEI List of NIS Experts compiled as a result of this procedure will be valid for a period of up to 4 years. The CEI will remain open to new applications for this whole period until 3 months before the end of the 4th year. Regular evaluations of new applications will be conducted in order to update the List of NIS Experts.

7. ESTIMATED BUDGET

It is anticipated that a budget of approximately €200.000,00 will be made available in 2018 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 the European Commission's standard 'Daily allowance' or *per diem* rates for each European Country. Please note that in EU countries where the tax laws stipulate a withholding tax from self-employed consultants, then ENISA will fully comply with this obligation.

If the expert is from a location other than the location required for the provision of services or place of meeting, the following expenses are then eligible:

- 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.

- A '*per diem'* applicable to the country in which the consultancy or 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 is intended to cover all daily living expenses including hotel, meals, local travel etc.

- No other claims for living or transportation costs will be accepted.

Each specific project for which an applicant may be asked to participate in, can have a budget up to a maximum of **€9.900,00** which equates to 22 working days at 8 hours per day. In accordance with EU procurement rules, a maximum amount of **€15,000.00** (including costs) can be paid to any individual expert during the course of one calendar year **by direct award**.

Each subject matter expert will be selected and involved **per project.** It may be possible under certain circumstances for a subject matter expert to be selected for more than one project in a calendar year by direct award, as long as the projects are from different Activity Objectives.

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 NIS Experts in 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 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 NIS 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.