Call for Expressions of Interest

ENISA P/09/09/CEI

"EXPERTS FOR IDENTIFYING EMERGING AND FUTURE RISKS POSED BY NEW ICTS"

ANNEX III

TECHNICAL DESCRIPTION - 2010

CONTENTS

TECHNICAL DESCRIPTION

1. INTRODUCTION

To achieve the desired impact and build on synergies, the Agency follows a multi-annual work plan. Each thematic programme (MTP) consists of several Work Packages (WPK) that include specific tasks and activities to implement the thematic programme. Work Programmes may also include Preparatory Actions (PAs), which are activities that are designed to be completed in one year and are used to determine whether or not a new MTP should be initiated.

The major thematic areas in which ENISA will be involved this year are presented below. For more information and for a detailed description, please refer to the ENISA Work Programme 2010 available here:
http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/enisa-work-programme-2010

MTP 1: Improving resilience in European e-Communication networks

In 2008, this MTP focused on stocktaking, best practices identification and analysis of gaps of measures deployed by both National Regulatory Authorities (NRAs) and network operators and service providers. MTP 1 also analysed the suitability of currently deployed backbone internet technologies regarding integrity and stability of network. In 2009, MTP 1 compared the findings against similar international experiences and results, issued guidelines, and finally formulated consensus-based recommendations after broad consultation with concerned stakeholders. In 2010, the main effort in this area will be to support the actions described in the recent communication on CIIP released by the Commission in March 2009.

MTP 2: Developing and maintaining co-operation between Member States

In 2008 the MTP aimed at a) the identification of Europe-wide security competence circles on topics such as Awareness Raising and Incident Response, b) the European NIS good practice Brokerage. In 2009, NIS capacity building for micro enterprises was added for the duration of one year. In 2010, further co-operation among Member States will be developed further and international cooperation opportunities will be explored with the aim of improving the capabilities of all Members States and increasing the overall coherence of the approach to NIS at the pan-European level. Due to its limited resources, the Agency will cooperate closely with the Commission services in order to minimize its efforts and maximize the results.

MTP 3: Identifying emerging risks for creating trust and confidence

The Agency has established a framework that will enable decision makers to better understand and assess emerging risks arising from new technologies and new applications. One of the principal goals of this framework is to help stakeholders' develop mutual trust and confidence in dealing with emerging risks. To this end, the Agency developed a proof of concept in 2008 of a

European capacity for the evaluation of risks that may emerge in 2 to 3 years ahead, linked to a Stakeholder Forum for multi-stakeholder dialogue with public and private sector decision makers. In 2009, this proof of concept was tested and developed further with the aim to deploy it with Member States in 2010. The Agency will continue preparing Risk Assessment reports to express the Agency's view on emerging risks arising from new technologies and new applications. In addition, the Agency will explore topics related to accountability and trust in the future Internet. As such, this MTP should provide an antenna function for decision makers in Europe and possibly beyond.

PA1: Identity, accountability and trust in the future Internet

Following recent developments of the Internet, in parallel to their real life, each person has the opportunity of living additional lives in the virtual world. A trend observed over the last few years, first in the research community, but now also in commercial offerings is the increase of interactions between these two worlds, making real-world information accessible to services on the Internet. A parallel development is the so-called Internet of Things (IoT) which, as an evolution of today's RFID technology, consists of networks of actuators and sensor nodes that interact with objects bearing tags. As a response to these developments, the overall goal of this Preparatory Action is to "ensure that Europe maintains a high level of security and confidence of both users and industry on the ICT infrastructure and provided services, while at the same time limiting the threats to civil liberties and privacy".

PA2: Identifying drivers and frameworks for EU sectoral NIS Cooperation

As intangible assets have become increasingly core to companies' value, general economic and operational incentives for the development of public-private cooperation in tackling NIS challenges are increasingly required. Traditional forms of protection are no longer enough to prevent intruders from entering and stealing or damaging key assets and a more proactive approach is needed. This approach should encompass an overall framework of organisational differentiation between public and private actors and along organisational supply chains, based on a realistic assessment of various parties' ability to tackle NIS challenges, taking into account their legitimate commercial or public service responsibilities and capabilities.

The purpose of this PA is to clarify the question of how to get commitments from relevant actors to collective action to address NIS challenges at a pan-European level.

2. REQUIREMENTS FOR SUBJECT MATTER EXPERTS

In implementing the afore-mentioned work programme, ENISA will need to seek assistance from external subject matter experts to participate in specific projects and provide their expertise and contribution *across the various thematic programmes (MTP) and Work Packages.*

Specifically for Work Package 3.1, ENISA envisages that subject matter experts will be required for the following activities:

2.1 MTP3 – *WPK 3.1: Framework for assessing and discussing emerging and future risks - Analysis of specific scenarios*

In the context of this work package, and in continuation with last year's assessments on Cloud Computing, eID, Internet of Things / RFID, Data mining / Profiling, ENISA will perform two risk assessments of emerging and future risks in 2010, following the similar approach we have followed in our previous assessments (for more information, please refer to the ENISA Work Programme 2010, where the MTP3 is described in detail). The two scenarios for the assessments will be on:

- **Trust and Privacy**: we will be looking to identify major risks in the area of trust, security and privacy posed by new and emerging technologies and applications.
- **Resilience**: here we will seek to identify risks and positive impacts on communication networks, services and systems resilience arising from the implementation of emerging technologies and applications.

In each of these two scenario assessment projects, we will be setting up an expert group of approximately 12-15 subject matter experts, as we did last year. The experts will be expected to follow the ENISA EFR Framework, in order to perform the risk assessment activities; this will depend on the particular field and stage of the assessment they are selected to participate. Specifically, subject matter experts will contribute to the identification and definition of:

- Scenarios
- Assets
- Threats and Vulnerabilities
- Final risks
- Controls / Safeguards and Recommendations

It is noted that the responsible for co-ordination from ENISA would provide appropriate details at the beginning of the project. For more information on the EFR Framework, please refer to EFR Introductory Manual (see Annex IV).

In terms of meetings, two or three face-to-face meetings are envisaged per each risk assessment project, while the coordination of the activities of the group is going to be performed mainly remotely (e.g. teleconferencing, video conferencing etc.), in order to facilitate discussions among all experts. In addition to this, a dedicated mailing list for each risk assessment is going to be established and used as the major communication channel for the expert group of each risk assessment. It should also be noted that a dedicated portal / workspace to facilitate

communication and collaboration of the ENISA virtual expert groups is actually under development; so in addition to all the communication and collaboration methods mentioned above, this workspace is also expected to be used in due course. More information on this will be communicated at a later stage to the selected experts.

2.2 MTP 1 – *WPK 1.3: Improving resilience in European e-communication networks. Investigation of innovative actions*

For 2010 ENISA will extend its work on assessing the impact of networking trends to the resilience of public communications networks by identifying and promoting architectural design principles that result in true end-to-end (e2e) security. For this purpose, external experts with relevant expertise in the following fields are required:

- Resilience of Communications Networks;
- Network technologies (including Domain Name System) with regard to security.

Please refer to WPK1.3 in ENISA Work Programme for 2010, page 14 of the document (available at: http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/enisa-work-programme-2010).

2.3 PA1: *Identity, accountability and trust in the Future Internet*

On-line services, applications and transactions can assure benefits and competitive advantage for citizens and the European economy. However, this cannot be achieved without safeguarding the integrity of the information, protection of the source of information, the genuine authentication (of entities or data, where required), establishment of trust (with persons, as well as objects and actuators) and at the same time protecting the personal data and securing the privacy of the individuals.
In the context on PA1, for 2010, we will address two topics with the support of external experts:

(1) Electronic identity in online environments (including eID, Federated identity, RFID, avatars, etc.). Please refer to PA1.1 work package in ENISA Work Programme for 2010, page 35 of the document (available at: http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/enisa-work-programme-2010).
(2) Trust, Accountability and Privacy. Please refer to PA1.2 work package in ENISA Work Programme for 2010, page 37 of the document (available at: http://www.enisa.europa.eu/about-enisa/activities/programmes-reports/enisa-work-programme-2010).

3. AREAS OF EXPERTISE SOUGHT

Based on the requirements presented in Section 3 above, ENISA seeks to establish a list of subject matter experts, from which experts will be selected to assist the Agency in carrying out the work activities foreseen in its Work Packages.

The following is a non exhaustive list of fields for which expertise may be sought:

- **Technical expertise in ICT and emerging application areas;** specifically in the following areas:
  - Virtualisation technologies / Cloud computing
  - Internet of Things/ Future Internet / Ubiquitous environments / Ambient Intelligence: mobile technologies, location-based services, RFID, etc.
  - Data mining and profiling techniques
  -"Electronic identity" and related technologies: electronic authentication, authentication protocols, smart cards, electronic ID cards and passports Federated identity, RFID, avatars, etc
  - Resilience of Communications Networks
  - Network technologies (including Domain Name System) with regard to security
  - Applied cryptography: algorithms, protocols, standards
  - Trust & Accountability
  -Emerging application areas not covered by the above mentioned technologies: e.g. transportation and automotive, eGovernment, eHealth, etc.
- **Information security**:
  - Information security considerations regarding the above-mentioned technologies (e.g. vulnerabilities, threats, threat agents, etc.)
  - Information security risk management: Expertise and experience in conducting risk assessment and risk management exercises, using appropriate risk management methodologies and tools
- **Legal & ethical expertise** related to IT issues, in particular IT security, privacy and data protection
- **Social expertise**: Social implications of ICT and information security
- **Economic expertise**: Economic implications of ICT and information security

4. TASKS AND ACTIVITIES OF THE SUBJECT MATTER EXPERTS

The subject matter experts will 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.
- Participate in any face-to-face meetings and teleconferences organised.
- Act as an ambassador for ENISA activities (e.g. disseminate the results to their affiliations and organisations, report in various events/presentations, etc.).

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

5. SELECTION CRITERIA

Applicants will be evaluated according to their technical and professional capacity, following the criteria below:

- Relevance of their current job responsibilities, their expertise and experience (please see Section 3, e.g. social, economical, legal etc.)
- Previous participation in similar activities; in particular, participation in relevant EU projects would be an advantage.
- English as a working language

Proof must be provided of the technical and professional capacity of the applicant on the basis of the following:

- Evidence of their educational and professional qualifications. **Curriculum vitae must be provided**, preferably in the EU format, the template can be downloaded from the following web link: (http://europass.cedefop.europa.eu/img/dynamic/c1344/type.FileContent.file/CVTemplate_en_GB.doc)
- Applicants should provide a list of related projects that they have carried out over the past 3 years.
- Languages covered by the applicant should be indicated.

6. DURATION OF THE LIST of EXPERTS

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

7. ESTIMATED BUDGET

It is anticipated that a budget of approximately €120,000 will be made available in 2010 for the various projects covered by this CEI. Each selected Expert will be remunerated with a **fixed fee of €450 per man-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.

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 living or transportation costs will be accepted.

A maximum of **€5,000.00** per year (including costs) can be paid to an 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 separate MTPs.

Please note that for any particular project which may require expenditure of amounts larger than €5,000.00 per Expert, 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 CEI List of Experts in a particular field/sub field, will be eligible to provide an offer for their services.

It is also noted that applicants that do not wish to be remunerated are also eligible to apply for inclusion in the CEI List of Experts, and they should indicate 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 face-to-face meeting, should they wish to be reimbursed.