VACANCY NOTICE

NATIONAL EXPERTS SECONDED TO ENISA

REF. ENISA-SNE-2013-09

Applications are invited for the establishment of a **reserve list of National Experts** to be seconded to the European Union Agency for Network and Information Security.

The Agency

The European Union Agency for Network and Information Security was established by the European Parliament and the Council Regulation (EU) No 526/2013 of 21 May 2013 (OJ L 165/41, 18.06.2013)[1] in order to assist the Union in ensuring a high and effective level of network and information security. The Agency shall contribute to the development of a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union.

ENISA shall assist the Commission, the Member States and the business community in meeting the requirements of network and information security, including those of present and future Community legislation.

The Agency will facilitate the development of a culture of security that builds on solid education and training foundations, awareness and best practices, and that encourages individuals, business and public administrations to actively participate in the protection of their information technology and network facilities.

In establishing and promoting this holistic approach to security, the Agency's activities shall be focused along five main axes:

- collecting and analysing data on security incidents and emerging risks in Europe;
- assisting and advising the Commission and the Member States in their dialogue with industry to address security related problems and, when called upon, in the technical preparatory work for updating and developing Community legislation in the field of network and information security;
- promoting best practices, risk assessment and risk management, training and awareness raising actions;
- encouraging co-operation between different actors, developing and maintaining contact with institutions, the business community and consumer organizations, notably through public/private partnerships;
- tracking the development of standards for products and services in the field of network and information security and promoting their use.

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF

ENISA is located in Heraklion (the agency's official seat) with an operational office in Athens (Greece). The place of employment for the Seconded National Expert is Athens. ENISA's staff are expected to be reasonably mobile in order to respond to the needs of the Member States on the basis of planned as well as ad hoc needs. Applicants will be expected to travel in line with the requirements of the assignment for which they are employed.

The Agency offers an attractive arrangement of flexible working.

Further information about ENISA may be found on our website: http://www.enisa.europa.eu/

Job Description

ENISA is looking for Seconded National Experts in the field of Network and Information Security (NIS) that will be requested to support the Agency's Core Operations Department in three different areas of expertise such as:

- **Cyber Crisis Exercises and Cooperation[2],**
- **Critical Information Infrastructure Protection[3],**
- **Computer Emergency Response Teams (CERTs, aka CSIRTs)**

The successful candidates will be responsible for the following tasks:

- Support and manage the preparation of workshops and conferences.
- Collecting information and knowledge on scenarios, incidents, and good practices in the area of Network and Information Security.
- Perform stock taking, survey experts, analysis and develop recommendations in different areas of Network and Information Security, in line with the needs of the work programme of the Agency.
- Identify relevant stakeholders, form expert groups and manage them including steering and editing technical content.
- Setting up and management of tenders and contracts related to the above topics
- Contribute to the dissemination and take up of the results of the Agency.

Qualifications and experience required:

a) Formal requirements:

- A level of education which corresponds to completed university studies attested by a diploma when the normal period of university education is four years or more, or a level of education which corresponds to completed university studies attested by a diploma and appropriate professional experience of at least one year when the normal period of university education is at least three years;

[2] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation
[3] http://www.enisa.europa.eu/activities/Resilience-and-CIIP

- In addition to the above, 3 years of professional experience in the Network and Information Security field relevant to the duties concerned, after the award of the university degree;
- Thorough knowledge of one of the official languages of the European Union and a satisfactory knowledge of another official European language;
- Be a national of a Member State of the European Union and the EFTA countries.

b) Selection criteria:

Essential

- University degree in applied sciences, such as for example Computer Science, Electrical/Electronics Engineering, Sciences or Mathematics, etc.
- Proven experience in the areas mentioned in the job description
- Good understanding in the latest regulatory/policy developments (at EU level) regarding the above mentioned areas.
- Good analytical, communication and presentation skills (the ability to present results in public and in clear written English).
- Ability to work under pressure and maintain a professional demeanour while managing his/her responsibilities.
- Good inter-personal skills and capacity to work effectively within a team.
- Good knowledge of written and spoken English
- Work experience in a multicultural environment.
- Experience with project management and self-responsible work.

Advantageous:

- Proven experience in the areas of
    - cyber incidents
    - supporting the design, planning, conduct and evaluation of cyber incident/crisis exercises.
    - Experience in (preferably international) projects on topics related to cyber exercises, simulation/emulation infrastructures, incident management and reporting, situational awareness, public private partnerships;
- Proven professional and hands-on experience in
    - Following essential IT security news sources on a regular basis, via several channels including social networks and/or Twitter
    - Identification of mid- and long term trends, threats and risks related to that area
    - Compilation of that data and transforming it into meaningful advice for various target groups about those topics (If you ever worked in an active CERT, and were involved in the creation of security advisories and whitepapers, we consider the above as given)
    - Very good understanding of (and preferably hands-on experience with) the crucial CERT services like incident response or alerting & warning
    - Very good understanding of network and related technologies, tools and protocols
    - Clearance to handle information up to the level of EU-SECRET

- Hands on experience (in operational and/or research environments) preferably in one or more of the following topics
    - incident reporting mechanisms
    - internet resilience and internet interconnections
    - ICS-SCADA and Smart Grids
    - internet interconnected networks
    - Cloud Computing
    - Mobile Applications
    - Inter banking transactions
- Experience in identifying and developing good practices in the area of communication networks and services;
- Experience with IT tools including office applications, databases, web-platforms such Sharepoint, virtualization environments, etc.
- Previous publications addressing the above mentioned topics. List(s) of publications should be included;
- Very good understanding of the European and national policy agendas in the area of security and resilience of communication networks;
- Experience in managing relationships with external partners (e.g. vendors, providers).
- Experience in designing and implementing security solutions in an operational environment.
- Experience in liaising with policy making, political, regulatory and standardization bodies
- Familiar with the European institutions.
- Good knowledge of the relevant international standardization landscape.

Conditions of secondment

The National Experts will be seconded to the Agency for a period of minimum 1 year with the possibility of renewal up to four years. The secondment will start as soon as a position is available according to ENISA needs.

Submission of applications

In order for an application to be considered valid, candidates are requested to submit to their Permanent Representation to the European Union in Brussels the following documents:

- Detailed **curriculum vitae in European format** available on the following website: http://europass.cedefop.europa.eu/

- **Letter of motivation** (1 page maximum)

When sending their applications, candidates are requested to specify for which area of expertise they wish to apply among the following:

- **Cyber Crisis Exercises and Cooperation[4],**
- **Critical Information Infrastructure Protection[5],**
- **Computer Emergency Response Teams (CERTs, aka CSIRTs)**

[4] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation
[5] http://www.enisa.europa.eu/activities/Resilience-and-CIIP

The applications including CV and letter of motivation should be sent preferably in English. Applicants may contact the Ministry of Foreign Affairs in their own country in order to obtain the contact details of the Permanent Representation to the European Union in Brussels.

This call for seconded national experts will remain open until 30 June 2014 at 14:00 (Greek local time). The first selection for secondment will take place no earlier than two months following the publication of this vacancy notice. Further evaluations will be carried out as necessary to fill possible on-going needs according to the number of applications received.

Published on ENISA website: 14/10/2013