NATIONAL EXPERTS SECONDED TO ENISA  
Ref. ENISA-SNE-2010-01

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

The Agency


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. In particular, its 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.

The headquarters of ENISA is Heraklion, Crete (Greece).

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

---


The **Seconded National Experts** will be requested to support the Agency’s operational departments in the implementation of its yearly work program notably for the development of technical areas such as risk analysis and management, security policy, security tools and architecture, awareness raising, relations with industry and international institutions, cooperation with Member States and European Bodies, computer incident and response handling policy.

The operational department and the respective expertise required for its units are as follows:

**Risk Analysis and Management:**

This section evaluates the current and emerging risks, the risk assessment and management methods and tools currently used or under development, how they are, or should be, integrated into the general business governance and how they can contribute to the IT business continuity.

**Job description:**

- Good knowledge of Risk Assessment of applications and technologies
- Good knowledge of protection and risk mitigation strategies
- Good knowledge continuity strategies and measures
- Experience with scenario building and analysis
- Experience with management of projects and groups of experts

**Security Policy:**

This section is concentrating on the evaluation of current security policies (operation impact of European policies on eSignature, eligibility management, Privacy, security and resilience of eCommunication systems) and advice on possible improvements.

**Job description:**

- Good understanding of policy, organisational and/or technical problems related to security and resilience of communication networks
- Good experience in designing, planning or executing national or regional exercises in the area of resilience of communication networks
- Proven multidisciplinary professional experience with emphasis on policy analysis and development and technical background in computer sciences/engineering
- Proven experience in managing projects and groups of experts, very good ability to synthesize opinions and build momentum
- Proven experience in collecting and analysing data and drafting reports,
- Very good communication, presentation and team work skills
Security Tools and Architectures:

This section is concentrated in networking technologies and protocols and the latest trends in ICT, such as Future Internet, Internet of Things, sensor networks, etc. and understanding of their implications in terms of resilience, privacy and trust. At the same time follows relevant standardisation activities in the areas of interest (e.g. resilience).

Job description:

- Deep knowledge of networking architectures (fixed and wireless) and protocols, security enhancing technologies and tools and security auditing tools.
- Knowledge of latest trends in ICT, such as the Future Internet, Internet of Things, sensor networks, etc, and understanding of their implications in terms of privacy and trust.
- Understanding on emerging risks and threats arising from the introduction of new technologies from the perspective of improving resilience (of communications networks), privacy and trust.
- Understanding of the technical building blocks of security in networked systems such as public and secret key encryption, key establishment protocols, authentication, confidentiality and integrity mechanisms.
- Familiarity with development of standards and with European/international standardisation bodies.
- Good analytical capability.
- Experience in drafting reports.
- Experience with management of projects and working groups of experts.
- Good experience in collecting and analysing data.

Awareness Raising:

This section aims at collecting best practices on how to organise and measure information security awareness campaigns with various target audiences and is currently developing a European awareness raising community.

Job description:

- Good understanding of awareness raising methods and best practices devoted to improving the culture and practice of network and information security throughout Europe.
- Ability to facilitate network and information security education and training in Europe.
- Experience in supporting ad-hoc Working Groups set up in this field of expertise.
- Experience with management of projects.
- Experience in drafting report.
- Good experience in collecting and analysing data.
**Computer Incident Response Handling Policy:**

The section aims at collecting best practices for computer incident response teams and works closely together with the CERT community to promote best practices and trainings.

**Job description:**
- Good knowledge of NIS with regards to operation and implementation
- Good knowledge of internet protocols
- Basic knowledge of sensor network technology
- Basic knowledge of data correlation

**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;
- 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**
- Proven experience in the areas mentioned in the job description.
- Good knowledge of both written and spoken English.
- Experience with project management and self-responsible work.
- Excellent written communication & presentation skills.
- Strong inter-personal skills and ability to work well in a team.
Advantageous:

- Experience in dealing with NIS projects.
- Experience in managing relationships with external partners (e.g. vendors, providers).
- Familiar with the European institutions.

Conditions of secondment
The National Experts will be seconded to the Agency for a period of minimum six months 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/](http://europass.cedefop.europa.eu/)
- Letter of motivation (1 page maximum)

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.

The closing date for the submission of applications is 31st March 2010. The Agency will only take into account applications sent by the Permanent Representations before the deadline.

Applicants shall liaise with their Permanent Representation to ensure that their application reaches the Agency well on time.

Published on ENISA website: 22/02/2010