VACANCY NOTICE

For the establishment of a reserve list of:

EXPERTS IN NETWORK AND INFORMATION SECURITY (AD6)

Ref. ENISA-TA-AD-2012-06

Applications are invited for the establishment of a reserve list for: **Experts in Network and Information Security** at the European Network and Information Security Agency.

The Agency

The European Network and Information Security Agency was established by the European Parliament and the Council Regulation (EC) No 460/2004 of 10 March 2004 (OJ L 77, 13.3.2004)[1] in order to assist the Community in ensuring a high and effective level of network and information security. The Regulation (EC) No **1007/2008**[2] of the European Parliament and of the Council of 24 September 2008 amended the Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration. 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

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:293:0001:0002:EN:PDF

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 seat of ENISA is Heraklion (Greece). The Agency Staff is 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 working.

The Agency offers an attractive arrangement of flexible working.

ENISA also has a branch office in Athens. Further information about ENISA may be found on our website: http://www.enisa.europa.eu/

Job description

ENISA is looking for experts in the field of Network and Information Security (NIS) in two different areas of expertise such as:

- **Privacy and Trust** (https://www.enisa.europa.eu/act/it) and in the area of:
- **Critical Information Infrastructure Protection**,

within the Technical Competence Department of ENISA, but must have the ability and willingness to contribute to such areas of the ENISA work programme, as Resilience, Security and Privacy, Risk, Secure applications, in line with the work program of the Agency.

The successful candidate will contribute to the team work performed in those areas; in order to achieve the objectives of the work program of ENISA[3]. He/she will participate in projects addressing the following tasks:

PRIVACY AND TRUST

Main responsibilities in the area of Privacy and Trust:

- Following up Research & Development projects related to Privacy and Trust as well as Network and Information Security technologies and identifying emerging trends.
- Following up technical developments in relevant international and European standardisation bodies and technical committees and their liaising with ENISA.

[3] http://www.enisa.europa.eu/activities

- Liaising with other operational teams of ENISA on the policy and social implications of new security technologies.
- Setting up, supporting and managing ad-hoc working groups in his/her field of expertise.
- Collecting information and knowledge on security policies, good practices, and measures in areas of Network Information Security.
- Working with stakeholders to identify opportunities for brokering experience and good practice between Member States. Assisting Member States in capitalising on these opportunities by seeking to match requirements with available experience. Ensuring that brokerage activities have clear objectives and that these objectives are met.
- Contribute to the dissemination and take up of the results of the Agency.

CRITICAL INFORMATION INFRASTRUCTURE PROTECTION:

The **Expert in Critical Information Infrastructure Protection** will initially work in the Resilience and Critical Information Infrastructure Protection (CIIP) Unit of ENISA, but must have the ability and willingness to contribute to other areas of the ENISA work programme as and when required. Allocation of tasks is based on an internal work plan developed by the Agency.

The Resilience and CIIP unit of ENISA[4], among others, assist National Regulatory Authorities to implement national mandatory security incidents, develops security measures and good practices for ICS-SCADA and Smart Grids, Cloud Computing, and interconnected networks. It also organises pan European cyber security exercises and assists Member States in developing cyber contingency plans. Finally the unit manages the Pan European Public Private Partnership (PPPs) for Resilience and assists Member States in developing national PPPs.

Main responsibilities in the area of Critical Information Infrastructure Protection:

- Collecting information and knowledge on security policies, good practices, measures and standards in the areas of the Resilience and CIIP unit as defined above,
- Perform stock taking, survey experts, analyse and develop recommendations in different areas of the Resilience and CIIP unit, in line with the needs of the work programme.
- Identify relevant stakeholders, form expert groups and manage them including steering and editing technical content, organise workshops and validate findings.
- Set up and manage tenders and contracts related to the studies of the Resilience and CIIP unit.
- Contribute to the dissemination and take up of the results of the Resilience and CIIP unit and the Agency.

[4] http://www.enisa.europa.eu/act/res

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 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.

In addition, in order to be eligible a candidate must:

- Be a national of one of the Member States of the European Union;
- Be entitled to his/her full rights as a citizen[5];
- Have fulfilled any obligations imposed by the applicable laws concerning military service;
- Be physically fit to perform the duties linked to the post[6].

b) Selection criteria for the area of **Privacy and Trust:**

Essential

- Proven professional experience in the tasks described above.
- Very good understanding of policy, organisational and technical issues in the field of privacy and trust as well as Network and Information security.
- Understanding of data protection and privacy framework in Europe
- Understanding of security in fixed and wireless systems as well as internet architecture.
- Proven research experience on networking architectures extending beyond the transport layers covering also application layers.
- Knowledge of latest trends in ICT, such as Internet of Things, IOT, sensor networks, etc, and understanding of their implications in terms of 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.
- Knowledge of standard technical security tools used for encryption, filtering, intrusion detection and security audit.
- Familiarity with development of standards and with European/international standardisation bodies.
- Good analytical skills.
- Good communication skills and service-oriented attitude.

[5] Prior to the appointment, the successful candidate will be asked to provide a certificate issued by the competent Member State authority attesting the absence of any criminal record.

[6] Before appointment, the successful candidate shall be medically examined in line with the requirement of Article 28(e) of the Staff Regulations of Officials of the European Communities.

- Self-motivated and self-reliant in managing tasks.
- Good inter-personal skills and capacity to work effectively within a team.
- Good knowledge of both written and spoken English.
- Excellent oral and written communication skills.

Advantageous

- Hands on experience (in operational and/or research environments) encryption, key establishment protocols, authentication, confidentiality and integrity mechanisms. Also similar experience in Privacy Enhancing Technologies (PET) will be considered an asset.
- Good understanding in the latest regulatory/policy developments (at EU level) regarding the above mentioned areas.
- Familiarity with resistance of communication networks to attacks and their operational stability and continuity.
- Knowledge of R&D activities in Europe on network and information security, both policy-wise and content-wise.
- Experience in the European institutions and technical bodies relating to information security.
- Experience in designing and implementing security solutions in an operational environment.

c) Selection criteria for the area of **Critical Information Infrastructure Protection:**

Essential

- University degree in Computer Science, Engineering, or Natural Sciences
- Proven professional experience in the tasks described above, preferably in one or more of the following topics
    - incident reporting mechanisms
    - minimum security measures for ISPs and service providers
    - cyber security exercises and cyber contingency plans
    - good practices for ICS-SCADA,
    - Smart Grids
    - interconnected networks,
    - Cloud Computing
- Very good understanding of policy, organisational and technical issues related to the Security and Resilience of Communication Networks and Critical Information Infrastructures
- Good analytical skills
- Good knowledge of written and spoken English
- Strong communication skills (the ability to present results in public and in clear written English).
- Self-motivated and self-reliant in managing tasks

Advantageous

- Experience in identifying and developing good practices in the Security and Resilience of Communication Networks and Critical Information Infrastructures
- Experience in (preferably international) projects on the topics of the Resilience and CIIP Unit
- Experience in liaising with political and regulatory bodies as well as standardisation bodies
- Very good understanding of the European and national policy agendas in the area of security and resilience of communication networks

d) For both areas of expertise, the following skills will also be taken into consideration:

- Knowledge of and experience in project leadership and management.
- Presentation Skills.
- Ability to work under pressure and maintain a professional demeanour while managing his/her responsibilities.
- Work experience in a multicultural environment.
- Language skills.

Selection procedure

A reserve list for Experts in Network and Information Security will be drawn up which will indicate the area of expertise each candidate has been selected for. Candidates will be appointed to a position according to the needs of the Agency, on the basis of the reserve list of candidates, proposed by the Selection Committee and established following an open selection process involving interviews.

More specifically, the Selection Committee decides on those candidates who are admitted to the selection procedure in accordance with the requirements as specified in the vacancy notice. The applications of the candidates admitted to the selection procedure are reviewed and the Selection Committee decides on those candidates who are invited to attend an interview. The Selection Committee adheres strictly to the conditions of admission laid down in the vacancy notice when deciding whether or not candidates are to be admitted. Candidates admitted to a previous selection procedure will not automatically be eligible. Should the selection board discover at any stage in the procedure that the candidate does not meet one or more of the general or special conditions for admission to the selection procedure or that the information on the application form does not correspond with the supporting documents, the candidate will be disqualified. Candidates may be asked to undergo a written test; should this be the case candidates will be informed in advance. The activity of the Selection Committee ends with the drawing of a reserve list of suitable applicants to occupy the position advertised. Candidates should note that inclusion on the shortlist does not guarantee recruitment.

The reserve lists will be valid until 31/12/2013 and may be extended by decision of the Executive Director for a further 12 months. Each candidate will be informed by letter whether or not he/she has been placed on the reserve list. If a letter of intention is issued, the candidate must undergo a compulsory medical examination to establish that he/she meets the standard of physical fitness necessary to perform the duties involved and the candidate must provide original or certified copies of all relevant documents.

Following this procedure, a reserve list of a maximum of 10 candidates will be drawn up which might be used to recruit staff for positions in the areas referred to in this vacancy. The Selection Committee is nominated by the Appointing Authority and the Staff Committee; its work and deliberations are confidential and impartial. **It is strictly forbidden for the candidates to make any contact with the Selection Committee, either directly or indirectly. Any infringement to this rule will disqualify the candidate from the competition.**

All enquiries or request for information in relation to the competition should be addressed to the following email address recruitment@enisa.europa.eu

Data protection

The purpose of processing of the data you submit is to manage your application(s) in view of possible pre-selection and recruitment at ENISA. ENISA does not publish personal data of candidates. Personal data is processed by and accessible to authorised ENISA personnel. Personal data submitted is kept confidential. ENISA adheres to and is regulated under Regulation (EC) No 45/2001 on personal data. ENISA is supervised by EDPS, http://www.edps.europa.eu. For any further enquiries you may contact the Data Protection Officer at: dataprotection@enisa.europa.eu

Contractual conditions

The successful candidate will be recruited as a member of the temporary staff, pursuant to Article 2a) of the Conditions of Employment of Other Servants of the European Communities, for a period of three years renewable or until the end of the Agency’s mandate whichever is the earliest.

The appointment will be in grade **AD6.** Successful candidates, who are recruited, shall undergo an initial probation period of 6 months. For reasons related to the Agency's operational requirements, the successful candidate will be required to be available at the shortest possible notice.

Pay and welfare benefits

The pay of staff members consists of a basic salary supplemented with various allowances, including family allowances.

The indicative basic monthly salary[7] for grade AD 6, step 1, is **4,921.28 EUR**. Nevertheless, this basic salary is adapted through a series of allowances according to your personal situation (i.e. marital status, dependent children, not being national of the State hosting ENISA and not having habitually resided within the territory of that State during the five years ending six month before the staff member entered the service, etc.). The provisions guiding the calculation of these allowances can be consulted in Annex VII of the EU Staff Regulations available at the following address:
http://europa.eu/epso/discover/careers/staff_regulations/index_en.htm

Community Tax

The salaries of staff members are subject to a Community tax deducted at source. They are exempt from national tax on salary and are members of the Community social security and pension schemes.

For additional information about salaries, deductions and allowances please consult the Staff Regulations of Officials of the European Communities:
http://europa.eu/epso/discover/careers/staff_regulations/index_en.htm

Equal opportunities

ENISA is an equal opportunities employer and accepts applications without distinction on the grounds of sex, racial or ethnic origin, religion or belief, age or sexual orientation, marital status or family situation. Applications from women and disabled candidates are encouraged. The staff members are recruited on the broadest possible geographical basis from among nationals of all Member States of the European Communities.

[7] Basic Salary: there is a basic salary scale for each grade, divided into a number of steps. Staff members progress automatically to the next step every two years until they reach the top of the scale for that grade.
Allowances: In addition to their basic salary, staff members may be entitled to various allowances, in particular an expatriation or foreign residence allowance, and family allowances, including household allowance, dependent child allowance, pre-school allowance and an education allowance. Under certain circumstances, in particular where staff members are obliged to change their place of residence in order to take up employment, the Agency may also reimburse various expenses incurred on recruitment, notably removal expenses.

Complaints

If a candidate considers that he/she has been adversely affected by a particular decision, he/she can lodge a complaint under Article 90(2) of the Staff Regulations of Officials of the European Communities, at the following address:

ENISA
Attn: Human Resources
P.O. BOX 1309
71001 Heraklion, Greece.

The complaint must be lodged **within 3 months**. The time limit for initiating this type of procedure (see Staff Regulations as modified by Council Regulation No 723/2004 of 22 March 2004 published in the Official Journal of the European Union L 124 of 27 April 2004 – **http://eurlex.europa.eu**) starts to run from the time a candidate is notified of the act adversely affecting him/her.

Submission of applications

Information about the application procedure at ENISA may be found on our website: http://www.enisa.europa.eu/about-enisa/recruitment/application-procedure

Candidates shall carefully check whether they meet all formal requirements by the closing date for the submission of applications.

When sending their applications, candidates are requested to specify for which area of expertise they wish to apply.

The **closing date** for submission of applications is **Monday 1st October 2012.**

Published on ENISA website: Friday 31st August 2012