

EUROPEAN DEFENCE AGENCY (EDA)

Vacancy notice Agency's Seconded National Expert

Post	Project Officer Cyber Defence Technology
Type of post	SNE post (AD10 equivalent)
Management of staff	N.A.
Location	Brussels
Indicative starting date	01/05/2019
Level of Security Clearance	SECRET UE/EU SECRET
Closing date for applications	18/01/2019

In accordance with the Rules applicable to national experts seconded to the European Defence Agency(2016 / 1352), Seconded National Experts are seconded to the Agency while remaining in the service of their national employer and continuing to be paid their national salary by that employer. Therefore, in order to be considered in the selection process, candidates for an SNE post must be sponsored by their national authorities. Confirmation is required in the form of a letter of sponsorship addressed to the Agency as far as possible by the closing date for the receipt of applications; and in any case not later than the recruitment date. The Rules are available on the EDA website <http://www.eda.europa.eu - vacancies>.

The selection of candidates will follow the EDA Staff Recruitment Procedure. Candidates must apply for this post via the EDA website <http://www.eda.europa.eu - vacancies>. Please note that to make an EDA on - line application you will need to create your EDA profile using a valid e - mail address and a password.

1. BACKGROUND

The European Defence Agency was established on 12 July 2004, and is governed by Council Decision (CFSP) 2015/1835 defining the statute, seat and operational rules of the European Defence Agency.

The Agency has its headquarters in Brussels.

The main task of the EDA is to support the Council and the Member States in their effort to improve the Union's defence capabilities in the field of crisis management and to sustain the Common Security and Defence Policy (CSDP) as it currently stands and as it develops in the future.

The Agency is structured into four directorates. Three operational directorates: Cooperation Planning & Support; Capability, Armaments & Technology; and European Synergies & Innovation and the Corporate Services Directorate.

2. THE AGENCY'S WAY OF WORKING

The Agency is an “outward-facing” organisation, constantly interacting with its shareholders, the participating Member States, as well as with a wide range of stakeholders. It works in an integrated way, with multi-disciplinary teams representing all the Agency’s functional areas, to realise its objectives. Its business processes are flexible and oriented towards achieving results. Staff at all levels need to demonstrate the corresponding qualities of commitment, flexibility, innovation, and team-working; to work effectively with shareholders and stakeholder groups, formal and informal; and to operate without the need for detailed direction.

3. THE CAPABILITY, ARMAMENT & TECHNOLOGY DIRECTORATE

The Capability, Armament & Technology directorate prepares the programmes of tomorrow by maximising synergies between capabilities, armaments and Research & Technology. The Directorate brings together the Agency’s work in the areas of: Information Superiority (Communication & Information Systems, Surveillance & Reconnaissance, Space, Cyber Defence; Air (Remotely Piloted Aircraft Systems, Air-to-Air Refuelling, airlift and aerial systems technologies); Land and Logistics (Counter-IED, armoured systems, camp protection and land systems technologies, land systems, ammunitions, medical support and deployability); Maritime (Maritime Surveillance, Mine Counter Measures and naval systems technologies); and the Joint domain (mobility, transport, medical and Ammunition). Particular attention is given to identifying future Critical Defence Technologies needed to support military capabilities. The Directorate also provides PESCO secretariat functions.

4. DUTIES

The Project Officer Cyber Defence Technology will support the Head of Unit Information Superiority in developing research and technology opportunities for collaborative cyber defence projects.

In particular, the Project Officer Cyber Defence Technology will be responsible for the following activities:

- manage the activities of the Cyber Research and Technology (R&T) Ad hoc Working Group (AHWG) consistent with the Strategic Research Agenda and through preparing and managing studies and projects to support Member States;
- assist participating Member States (pMS) interested in the analysis and generation of projects, including through the development of related courses of action;
- contribute to the development of the relevant planning, coordinating with EDA’s Operational Directorates’ Units, to promote the coherence of the European defence capability landscape, with a focus on the cyber-related R&D dimension;
- support the validation and verification of requirements with stakeholders through prototyping projects, collaborative experimentation and participation in operational exercises;
- actively follow technology developments in the field of Cyber Defence and identify technology trends and solutions with respect to military requirements for Cyber Defence;
- provide input and advice to the EDA’s plans and financial management regimes, and externally to the Steering Board and other Member States’ meeting formats (Project Teams, Member States Points of Contact);
- manage information through EDA’s Collaborative Platform and Portfolio Project Management systems to maintain a high level of information sharing with Member States and internally within EDA;
- participate, on behalf of EDA, in conferences, seminars, and other activities within his/her subject matter expertise and deliver presentations and publications as required;
- deputise for the Project Officer Cyber Defence;

- additional tasks as required in the interest of the service;

Duties may evolve according to development of the EDA's structure and activities, and the decisions of EDA management.

5. QUALIFICATIONS AND EXPERIENCE REQUIRED

a. Conditions for eligibility

(1) General

- be a national of a Member State participating in the Agency;
- be entitled to his/her full rights as a citizen;
- have fulfilled any obligations imposed on him/her by the laws concerning military service;
- produce the appropriate character references as to his/her suitability for the performance of his/her duties;
- be physically fit to perform his/her duties;
- have a thorough knowledge of one of the languages of the participating Member States and a satisfactory knowledge of another of these languages to the extent necessary to discharge his/her duties;
- have no personal interest (financial, family relationship, or other) which could be in conflict with disinterested discharge of his/her duties within the Agency;
- hold a valid Personnel Security Clearance Certificate (national or EU PSC at SECRET UE/EU SECRET level). Personnel Security Clearance Certificate' (PSCC) means a certificate issued by a competent authority establishing that an individual is security cleared and holds a valid national or EU PSC, and which shows the level of EUCI to which that individual may be granted access (CONFIDENTIEL UE/EU CONFIDENTIAL or above), the date of validity of the relevant PSC and the date of expiry of the certificate itself. Note that the necessary procedure for obtaining a PSCC can be initiated on request of the employer only, and not by the individual candidate.);
- have 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 or be a graduate of a national or international Defence College; or where justified in the interests of the service, professional training of an equivalent level.

b. Essential selection criteria

(1) Professional

The candidate will be required to demonstrate that he/she has:

- excellent knowledge of technologies and experience of research activities related to Cyber Security and Cyber Defence;
- good knowledge of the Cyber Security industry;
- good knowledge of the international environment concerned with Cyber Defence;
- experience in the duties listed above;
- experience in managing projects;
- an understanding of the EDA's main tasks and functions;

- a very good knowledge of written and spoken English.

(2) Personal

All staff must be able to fit into the Agency's way of working (see para. 2). Other attributes important for this post include:

- organisational and negotiations skills;
- ability to work in a team in an international environment;
- results-orientation, and strong motivation;
- flexibility and innovativeness;
- commitment to the Agency's objectives;
- strong interpersonal, communication and analytical skills.

c. Desirable

The following will be considered an advantage:

- knowledge of the CSDP Capability Development Mechanism;
- experience of working in a multinational environment;
- hold a (recognised) Project Management qualification;
- hold a certification in the Information Assurance domain (eg CISSP, CCSP, CISA, CISM, etc...);
- experience within public security agency and/or in the security research organisation.

6. INDEPENDENCE AND DECLARATION OF INTEREST

The Project Officer Cyber Defence Technology will be required to make a declaration of commitment to act independently in the Agency's interest and to make a declaration in relation to interests that might be considered prejudicial to his/her independence.

7. APPOINTMENT AND CONDITIONS OF EMPLOYMENT

The Project Officer Cyber Defence Technology will be appointed by the Chief Executive.

Secondment will be as a member of the Seconded National Expert staff of the Agency for a three-year period (unless a shorter period is mutually agreed between the parties). Renewal is possible within the limits set out in the EDA SNE Rules. The successful candidates will be seconded as AD10 equivalent.

Applications are invited with a view to establishing a reserve list for the post of Project Officer Cyber Defence Technology at the EDA. This list is valid until 31/12/2019, and may be extended by decision of the Chief Executive. During the validity of the reserve list, successful candidates may be offered a secondment in the EDA according to their competences in relation to the specific requirements of the vacant post.

Inclusion on the reserve list does not imply any entitlement of secondment to the Agency.

8. EQUAL OPPORTUNITIES

The EDA is an equal opportunities employer and accepts applications without distinction on the grounds of age, race, political, philosophical or religious conviction, sex or sexual orientation and regardless of disabilities, marital status or family situation.

9. APPLICATION PROCEDURE

Candidates must submit their application electronically solely via the EDA website. Applications by any other means (hard copy or ordinary e-mail) will not be accepted. Applications must be submitted no later than midnight. Candidates are reminded that the on-line application system will not accept applications after midnight (Brussels time, GMT+1) on the date of the deadline.

When applying, candidates from Ministries of Defence or other governmental entities are encouraged to inform their national administration.

A selection panel will be appointed. Please note that the selection panel's internal proceedings are strictly confidential and that any contact with its members is forbidden.

Each application will be screened based on the requirements of the job profile stated in the vacancy notice. The most suitable applicants will be called for an interview and a written test.

If recruited, you will be requested to supply documentary evidence in support of the statements that you make for this application. Do not send any supporting or supplementary information until you have been asked to do so by the Agency.

Please note that once you have created your EDA profile, any correspondence regarding your application must be sent or received via your EDA profile.

For any prior enquiry, please refer to the FAQ (Frequently asked questions) section, or send an e-mail to recruitment@eda.europa.eu.

10. DATA PROTECTION

Please note that EDA will not return applications to candidates. The personal information EDA requests from candidates will be processed in line with Regulation (EC) N° 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. The purpose of processing personal data which candidates submit is to manage applications in view of possible pre-selection and recruitment at EDA.

More information on personal data protection in relation to selection and recruitment can be found on the EDA website: <http://www.eda.europa.eu/jobs/dataprotection>