JOB DESCRIPTION FORM SNE
SECDEFPOL.1 - job no. 273393

I. IDENTIFICATION OF THE JOB

Type of post:	Seconded National Expert (cost-free)
Job title:	Policy Officer (Cybersecurity and cyber defence)
Function group and grade bracket:	
Entity:	Security and Defence Policy Directorate Security and Defence Policy Division – SECDEFPOL.1 Cyber Sector
Specialised post:	Yes
Security clearance:	SECRET EU

II. TASKS

Under the authority of the Head of the Security and Defence Policy Division and as part of the Cyber Sector, the expert will deal with cyber security and cyber defence issues and his main tasks will include:

- support the EEAS with expertise in the EU policy making in particular with regard to ongoing processes and events in cyberspace issues such as the implementation of the EU Cyber Security Strategy, EU Cyber Defence Policy Framework; EU cyber defence issues and civil-military relations, facilitating the formulation of common EU positions etc;
- contribute to the elaboration and implementation of policies and activities to address external security threats to the EU in the area of cybersecurity and cyber defence;
- provide interface and follow up with Commission, Council, EP, EU agencies, Common Security and Defence Policy military actors and other relevant partners as well as with third parties in the areas mentioned above;
- contribute to the elaboration and further development of EU policies and activities in the area of cyber security, cyber defence and civil-military relations;
- prepare and/or contribute to policy documents related to this area, in close cooperation with geographic services and with other institutions, member states and international organisations, as appropriate, including inter-institutional decision-making process;
- contribute to developing awareness and capacities within the EEAS and other services, and provide policy guidance on cyber defence and civil-military relations;
- coordinate the implementation of the EU Cyber Security Strategy and Cyber Defence Policy Framework;
- contribute to the programming of the EU instruments to address cyber security and cyber defence issues;
- seek to ensure coordination, complementarity and synergies with measures under other thematic and geographic instruments as well as with CFSP actions;
- contribute to reports and briefings on activities in the area of responsibility;
- establish and maintain regular contacts and exchanges with other EU institutions, Member States, third countries, public and/or private international organisations and/or with research institutions and the academic community at large in the area of responsibility.

III. QUALIFICATIONS AND EXPERIENCE REQUIRED

- university diploma;
- Two years' relevant professional experience and ideally some professional experience in multinational organisations;
- have experience and knowledge of CFSP and CSDP;
- thorough knowledge of one EU working language and satisfactory knowledge of another one are required; in practical terms, in order to perform required duties, that means an excellent command of written and spoken English, in particular good report-writing skills; good knowledge of written and spoken French is desirable;
- good computer skills are essential, notably in word processing, spreadsheets, presentations software, Internet / Intranet and email systems. Knowledge of other IT tools would be an asset.

IV. CONDITIONS/ SKILLS REQUIRED

- have the ability to remain objective in complex scenarios and to display sensitivity and sound judgement;
- have good organisational skills, the ability to work under pressure and with tight deadlines and to manage multiple tasks and unexpected demands;
- have excellent drafting and communication skills;
- have excellent negotiating skills in a multinational environment;
- have the ability to work professionally as a member of the division, in mixed-composition task forces and working groups, in an interesting but challenging environment;
- maintain the highest standards of personal integrity, impartiality and self-discipline. The expert must exercise the greatest discretion with regard to all facts and information coming to his/her knowledge in the performance of his/her duties;
- national security clearance at SECRET UE level. Such clearance needs to be obtained from the competent authorities before secondment to the European External Action Service. It must be valid for the entire period of secondment. In its absence, the EEAS reserves the right to refuse the secondment as a national expert.

V. GENERAL CONDITIONS

National experts must be nationals of one of the Member States of the European Union and enjoy full rights as citizens.

The EEAS applies an equal opportunities policy.