

Seconded national expert
at the General Secretariat of the Council of the European Union

DGA 5 – Communication and Information Systems
(Ref.: END/2009/JAI/3)

Number of posts available: 1

Post available

Post at engineer/technical master's degree level within DG A 5 – Communication and Information Systems – of the General Secretariat of the Council of the European Union in Brussels (Belgium).

General

Decision 99/05 on the functions of DGA5 provides for the creation on 1 September 2005 of an INFOSEC section having responsibility for ensuring the security of classified information systems (at present around fifty in number). The activities of DG A 5's "Security of sensitive communication and information systems" unit centre on three sectors:

- ⇒ Study and validation
 - Drafting security documents
 - Security solutions and drafting of Security Management Procedures
 - Control and validation (VASSI)
- ⇒ Protection of networks
 - Technical supervision
 - Operations bureau
- ⇒ Operational management
 - Administration of encryption-related matters
 - TEMPEST laboratory
 - Support for those responsible for sensitive communication and information systems.

A. Tasks

Within the "Protection of networks" sector:

- organising contacts (CERT, judicial authorities, police authorities, other specialists);
- establishing incident management procedures (e.g.: confidentiality, communication, procedures for intervention following an attack, awareness-raising and training);
- establishing procedures for follow-up after the incident: documentation, improving defences, updating guidelines and procedures;
- active monitoring and implementation of changes to technical standards and the legislative framework for sensitive security information (SSI);

- putting in place means to gather information on computer and network vulnerabilities/alerts;
- putting in place ways of giving the alert;
- establishing a cell to watch for and analyse IT weaknesses and the threat they represent;
- establishing a cell to monitor technological developments.

B. Qualifications and experience required

- Candidates must have a full university education, attested by a diploma, or have equivalent professional experience;
- have performed functions relating to the monitoring of technological developments and the distribution of information in the service of a government, ministry, or national or international organisation having a role in security, **for at least five years**;
- have a sufficiently good knowledge of the French or English languages to be able to draft in one of those languages;
- be aware of procedures for the handling and follow up of security incidents;
- have knowledge of European standards and guidelines on SSI;
- have a sound knowledge of network, web and security architecture;
- have a good knowledge of technological research and monitoring tools in the SSI field;
- have knowledge of a risk analysis tool;
- have experience in seeking information in different media;
- have experience in the area of archiving;
- have experience in the area of the distribution of information;
- have experience in putting in place tools to monitor and accumulate information.

A few years' experience in a CERT (CSIRT) would be an advantage.

C. Requirements/skills

- Candidates must be able to assume a heavy workload and work effectively as a team member;
- have a sense of initiative and of organisation;
- have a national security clearance at a level equivalent to SECRET UE. Such clearance needs to be obtained from the competent authorities before secondment to the General Secretariat of the Council. The clearance must be valid for the entire period of secondment. In its absence, the General Secretariat reserves the right to refuse secondment as a national expert.

D. General conditions

- Candidates must be nationals of one of the Member States of the European Union and enjoy full rights as a citizen.

The General Secretariat of the Council is an equal opportunities employer.

**Seconded national expert
at the General Secretariat of the Council of the European Union
DGA 5 - Information and Communication Systems**

Ref.: END/2009/JAI/4

(1 post)

Job description

General

Decision 99/05 on the functions of DGA5 provides for the creation on 1 September 2005 of an INFOSEC section having responsibility for ensuring the security of classified information systems (at present around fifty in number). The activities of DGA5's "information and sensitive communications systems security unit" centre on three sectors:

- ⇒ Study and validation
 - Drafting security documents
 - Security solutions and drafting of Security Management Procedures
 - Control and validation (VASSI)
- ⇒ Protection of networks
 - Technical supervision
 - Operations bureau
- ⇒ Operational management
 - Administration of encryption-related matters
 - TEMPEST laboratory
 - Support to heads of sensitive information and communications systems

A. Tasks

Within the Operational Management sector:

- implementation of certification authorisations and the servers of the various systems used (Extranet, FADO, SOLAN, etc.) ;
- production of encryption keys for the systems under the responsibility of the General Secretariat of the Council ;
- pre-personalisation and personalisation of media used for keys or certificates (tokens, memory cards, etc.) ;
- initialising encryption equipment before installation ;
- installing encryption equipment ;
- locking encryption equipment ;

- support for users of encryption equipment ;
- participation in the procedures for purchasing encryption and security equipment ;
- participation in training courses relating to the management of encryption products.

B. Qualifications and experience required

- have completed secondary education attested by a diploma or have equivalent professional experience ;
- have performed functions relating to operational management of encryption systems for at least two years in the service of a government, ministry, national or international organisation having a role in security and defence ;
- have a sufficiently good knowledge of the French or English languages to be able to draft in one of those languages ;
- have experience in the implementation and operational management of IP encryption products (configuration, management centre) ;
- have, if possible, experience in the PKI (Public Key Infrastructure) field, in particular with regard to the following areas : X509, LDAP, PKCS, TLS, S/MIME ;
- have some knowledge of the LINUX family of operating systems, their settings and access restriction techniques ;
- have a thorough knowledge of networks (architecture, configuration of active elements) and their security (IPSEC).

A knowledge of encryption products (SECUNET's SINA or AEP's ED20x) would be an advantage.

An ability to use scripts combining OpenSSL and Perl on Windows and Linux platforms would also be an advantage.

C. Requirements/skills

- the ability to cope with a heavy workload and work effectively as a team member ;
- a sense of initiative and organisational ability ;
- a national security clearance level equivalent to SECRET UE. Such clearance must be obtained by the candidate from the relevant authorities before secondment to the General Secretariat of the Council. It must be valid for the entire period of secondment. In its absence, the General Secretariat reserves the right to refuse the secondment as a national expert.

D. General conditions

- The candidate must be a national of one of the Member States of the European Union and enjoy full rights as a citizen.

The General Secretariat of the Council applies an equal opportunities policy.

**National expert seconded (SNE)
to the General Secretariat of the Council of the European Union**

**EU Situation Centre (SITCEN):
Security Accreditation Authority (SAA) & Network Defence Capability (NDC) Team**

Job description

(Ref.: END/2009/JAI/5)

A. Tasks

- participating and contributing to the GSC internal task-force for the consolidation of the organisation, the missions, the perimeter of responsibilities and the interfaces of the GSC Network Defence Capability;
- exploring with the relevant services in Member States the practical operational cooperation schemes for cyber-attacks prevention and response;
- proposing solutions to develop and maintain awareness and preparedness of GSC senior officials with regards to cyber-threats and cyber-attacks;
- liaising with other SITCEN Units for developing internal synergies with regards to cyber-attacks prevention and response.

B. Required qualifications and experience

- have at least 5 years of technical & operational experience in cyber-defence;
- have exercised operational responsibilities in preventing and responding to cyber-attacks within a government or an international organisation;
- have experience in cyber-threats investigation;
- master the world-wide and European contexts with regards to the cooperation on computer Incident Response;
- be familiar with the European Security and Defence Policy;
- be open-minded and flexible;
- be a team player but with the ability to work autonomously and a strong sense of personal responsibility;
- have a working knowledge of English and French with drafting skills in one of these two languages. Other language skills would be appreciated.

C. Requirements

- SITCEN allows a degree of flexibility in working hours to adjust them to personal requirements.
- This post requires security clearance allowing access to classified documents (at EU TOP SECRET level). Such clearance must be obtained by the candidate from the relevant authorities before secondment to the General Secretariat of the Council. It must be valid for the entire period of secondment. In its absence, the General Secretariat reserves the right to refuse the secondment as a national expert.

D. General conditions

- Nationality of one of the Member States of the European Union and enjoyment of full rights as a citizen.

The General Secretariat of the Council applies an equal opportunities policy.
