



**Council of the European Union**  
General Secretariat

Directorate-General for Organisational Development and Services  
Directorate for Human Resources  
*The Director*

His/Her Excellency the Ambassador

Permanent Representative of the  
Member States to the  
European Union

(by e-mail)

Brussels, 8 November 2023

**Subject: Secondment to the General Secretariat of the Council of a national expert in the field of cyberintelligence**

Ref.: SNE/09/2023 (GSC.ORG.5.A.S1) - 1 post (379229)

Dear Sir or Madam,

The Safety and Security Directorate is seeking a cyberintelligence expert to support its Security Investigations and Counter-Intelligence team.

The job description is attached.

The duration of the secondment will be two years, with the possibility of extending it to a maximum of four years in total. Please note that in accordance with Article 5 of Council Decision (EU) 2015/1027, the secondment could be extended for an additional two years in exceptional cases.

The expert should take up their duties at the General Secretariat of the Council by **1 March 2024**.

The qualifications and experience required are set out in the annex.

The conditions of the secondment, including allowances paid by the Council, are set out in the Council Decision of 23 June 2015 concerning the rules applicable to experts on secondment to the General Secretariat of the Council (Council Decision (EU) 2015/1027, OJ L 163, 30.6.2015, repealing Decision 2007/829/EC). According to Article 2 of that Decision, seconded national experts must be nationals of an EU Member State. Member States are hereby invited to propose candidates for the post.

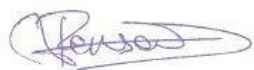
Proposals should indicate the national contact point(s) responsible for each candidate's submission. Submissions should be accompanied by a curriculum vitae detailing all posts held by the candidate to date as well as their education, and by a motivation letter.

Replies to this letter should be sent by email, no later than **17:00 CET on 30 November 2023**, to the following address: [sne.recruitment@consilium.europa.eu](mailto:sne.recruitment@consilium.europa.eu).

The relevant department, together with the Human Resources Directorate, will examine the applications received, decide which candidates to shortlist, and conduct the interviews. The Appointing Authority will decide on the appointment based on the outcome of the selection procedure. The General Secretariat of the Council may also decide to use the list of suitable candidates to fill future vacancies with the same profile.

If necessary, further information can be obtained from the General Secretariat of the Council by contacting Mr Philip Meulenberghs, Head of the Investigations and Threat Assessment Sector, tel. +32 (0)2 281 8034, email: [philip.meulenberghs@consilium.europa.eu](mailto:philip.meulenberghs@consilium.europa.eu).

Yours sincerely,



**Nathalie Pensaert**

## **Annexes**

Annex 1 – Job description

**Seconded National Expert (SNE)**  
**at the General Secretariat of the Council of the European Union**  
**Investigations and Threat Assessment (ORG.5.A.S1) – Cyberintelligence Expert**

Ref.: SNE/09/2023 (GSC.ORG.5.A.S1) - 1 post (379229)

**Job description**

**A. Main tasks and responsibilities**

Under the guidance of the Director of the Safety and Security Directorate (DSS) and the head of the Security Strategy and Business Continuity Unit, the expert will work in the unit's Investigations and Threat Assessment Sector's 'Security Investigation and Counter Intelligence Team'. The expert's direct line manager will be the Head of Sector – ORG5.A.S1 – Investigations and Threat Assessment.

The sector performs the full range of tasks connected with the management of security threats and risks: security investigations, open source and social media intelligence, security risk management, threat assessments, counter-intelligence activities, penetration testing, and awareness activities.

The sector provides senior management with security investigations analysis, risk and threat assessments, awareness briefings and advice on security.

The selected candidate is expected to perform the following tasks:

- The expert will work in a results-oriented, pragmatic and flexible manner. Depending on the dossier, the expert may work for the Head of Unit or the Director. The expert will have a lot of autonomy, but will be required to work in close cooperation and coordination with the counter-intelligence (CI) experts in the sector, the head of the Investigations Office and the team of security investigators, the open source intelligence (OSINT) and cybersecurity specialists, and the Cybersecurity Unit in the Digital Platforms directorate.
- The expert will help to coordinate the full range of activities connected with the investigation of cybersecurity incidents and risks. The expert will mainly deal with cybersecurity investigations and counter-intelligence.
- The expert will provide advice on cyber threats but will, in particular, have an operational role, coordinating and participating in cyber investigations, mapping cybersecurity incidents, and contributing to penetration tests and other tests and to cybersecurity studies, as needed.
- The expert will be asked to provide senior management with assessments, reports and advice in his or her area of expertise.

**B. Qualifications and experience**

Applicants should:

- have completed a university education, as evidenced by a diploma, or have equivalent professional experience;
- have at least five years – though preferably ten years – of professional experience in a state counter-intelligence function in a Member State's security service, with recent expert experience in the field of cyberintelligence;
- have expertise in state-sponsored cyberattacks (APT), the assessment of threat actors and their capabilities and motivation, and the assessment of the effectiveness of security threat mitigations against such actors;
- be able to link cyberintelligence with other forms of intelligence, including SIGINT and HUMINT;
- be able to translate complex technical IT concepts into understandable language for non-technical colleagues, investigators and management;
- be able to assess the impact of cyberattacks and describe this in written and oral briefings;
- be able to liaise and cooperate with the MS intelligence services in the field of cyber, and to interact with stakeholders in other GSC services, including the Cybersecurity Unit, the Digital Platforms directorate, the Data Protection Unit, and the Information Security Unit;
- have experience with cyber counter-intelligence briefings and advice and recommendations aimed at mitigating the threat of cyber espionage, raising awareness and reducing vulnerabilities;
- have experience with technical and forensic cyber investigations, and be able to conduct such investigations, giving comprehensible instructions to technicians, and translate the results into comprehensible reports for non-technical colleagues, investigators and management;
- have knowledge of the activities of the European institutions and the European intelligence structures and security services (knowledge of the EU's cyber policies would be considered an asset);
- have a thorough knowledge of one EU language and a satisfactory knowledge of a second EU language. In practice, in the interests of the service, the chosen candidate should have a thorough written and oral command of English and/or French. Accurate and analytical report writing ability in English or French is essential.

### **C. Conditions and skills required**

- Good drafting skills for the elaboration of drawing up analyses, reports and presentations on cyber security issues
- Ability to give briefings to various audiences including high-level managers
- Discretion in handling sensitive and confidential information
- Sound judgment skills in critical situations, as well as good multitasking skills
- Be versatile, well organised and able to prioritise and take the initiative
- Be a team player
- National security clearance at TRES SECRET UE/EU TOP SECRET level. Such clearance needs to be obtained by candidates from their relevant national authorities before being seconded to the General Secretariat of the Council. The clearance must be valid for the entire period of the secondment. If not, the General Secretariat reserves the right to refuse the secondment of the national expert.

#### **D. General conditions**

Applicants must:

- be nationals of one of the Member States of the European Union and enjoy full rights as a citizen;
- have fulfilled any obligations imposed by the law concerning military service.

The General Secretariat of the Council applies a diversity and inclusion policy.

Further information on the nature of the post can be obtained from Mr Philip MEULENBERGHS, Head of the Investigations and Threat Assessment Sector, tel. +32 (0)2 281 8034, email: [philip.meulenberghs@consilium.europa.eu](mailto:philip.meulenberghs@consilium.europa.eu).

---