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, 15 October 2021

Subject: **Secondment of a national expert - Cyber Intelligence - to the General Secretariat of the Council, GSC.ORG.5.A.S1, Safety and Security Directorate, Risk Management and Business Continuity Planning sector**

Ref.: SNE/07/2021 (379229)

Dear Sir/Madam,

The Safety and Security Directorate seeks a Cyber Intelligence Expert to support its Security Investigations and Counter Intelligence team.

The duration of the secondment is two years, with the possibility of extension to a maximum of four years in total. Please note that, in accordance with Article 5 of Council Decision 2015/1027/EC, this secondment could be extended for an additional period of up to two years in exceptional cases.

The qualifications and experience required are set out in the Annex. The expert should take up his or her duties at the General Secretariat of the Council by **1 February 2022**.

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

Member States are hereby invited to propose candidates qualified for this post.

I would be grateful if the proposals could indicate the national contact point(s) responsible for each candidate's submission. Submissions must be accompanied by a curriculum vitae providing details of education and all posts held until now, and by a letter of motivation.

Replies to this letter should be sent by e-mail, no later than **24 November 2021, 17.00 Brussels time,** to the following address: sne.recruitment@consilium.europa.eu.

The Safety and Security Directorate, together with the Human Resources Directorate, will examine the applications received, decide which candidates to shortlist, and conduct the interviews before 15 December 2021.

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 cover possible 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 (email philip.meulenberghs@consilium.europa.eu, tel. +32 2 281 8034).

Yours faithfully,

Nathalie Pensaert

Annex: 1

ANNEX

Seconded National Expert for
the General secretariat of the Council of the European Union

ORG.5.A.S1 - Risk Management and Business Continuity Planning

Cyber Intelligence Expert

(1 post)

Ref.: SNE/7/2021 (379229**)**

Description of post

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 Security Risk Management and Business Continuity Sector's "Security Investigation and Counter Intelligence Team". The expert's direct line manager will be the Head of Sector - ORG5.A.S1 - Security Risk Management and Business Continuity.

The sector is performing 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, awareness activities.

We provide senior management with security investigations, risk- and threat assessments, awareness briefings and advice about security.

The way of working for the expert will be result oriented, pragmatic and flexible. 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 he/she will be required work in close cooperation and coordination with the CI experts in the sector, the Head of the investigations office and the team of security investigators, the OSINT and cyber security specialists and network defence team in the "Digital Services" directorate.

The expert will help to coordinate the full range of activities connected with the investigation of cyber security incidents and risks. He/she will mainly deal with cyber security investigations and counter intelligence.

The expert will provide advice about cyber threats but will particularly have an operational role, to coordinate and participate in cyber investigations, to map cyber security incidents, to contribute to penetration and other tests and to cyber security studies as needed.

He/she will be asked to provide senior management with assessments, reports and advice in his/her domain of expertise.

B. Qualifications and experiences

Applicants should:

- have completed a full university education, as evidenced by a diploma, or have equivalent professional experience;
- have at least 5 but preferably 10, years' professional experience in a state counter intelligence function, in a member state security service, with recent expert experience in the field of cyber intelligence;

- expertise in state sponsored Cyber attacks (APT), the assessment of threat actors, their capabilities and motivation and of the effectiveness of security threat mitigations against those actors;
- have the ability to link cyber intelligence with other ways of intelligence, including Sigint and Humint;
- have ability to translate complex technical IT concepts into understandable language for non technical colleagues, investigators and management;
- have ability to assess the impact of a cyber attack and describe this in written and oral briefings;
- have the ability to liaise and cooperate with the MS intelligence services in the field of cyber, and to interact with stakeholders in other GSC's services, including the technical IT experts from the Network Defence capability, the IT directorate, and colleagues from the Information Security Unit in the Security Directorate;
- have experience with cyber-counterintelligence briefings and advice and recommendations aiming at mitigating the threat of cyber-espionage, raising awareness and reducing vulnerabilities;
- have experience with technical and forensic cyber investigations, ability to conduct such investigations, giving comprehensible instructions towards technicians and translate the result in comprehensible reports towards non technical colleagues, investigators and management;
- have a knowledge of the activities of the European institutions and the European intelligence structures and security services; knowledge about the Cyber policies of the EU would be considered an added value;
- languages: In practice, in the interests of the service, the chosen candidate should have a good knowledge in spoken and written English and/or French. Accurate and analytical report writing ability in English or French is essential. Knowledge of other EU member state languages, or Russian, Arabic or Chinese will be considered an advantage.

C. Conditions and skills required

- Good drafting skills for the elaboration of analysis, 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 to take initiatives;
- Be a team player;
- A national security clearance at TRES SECRET UE/EU TOP SECRET level. Such clearance needs to be obtained by the candidates from their relevant national authorities before secondment to the General Secretariat of the Council. The clearance must be valid for the entire period of secondment. If not, the General Secretariat reserves the right to refuse the secondment as national expert.

D. General conditions

- Nationality of one of the Member States of the European Union and enjoyment of full rights as a citizen.
- Have fulfilled any obligations imposed by the laws concerning military service.

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

For more information related to the selection, please contact Mr. Philip MEULENBERGHS: tel.+32.2.281 8034, e-mail: philip.meulenberghs@consilium.europa.eu