NOTIFICATION OF A "G10" GRADE VACANCY
OPEN TO NATIONALS OF NATO MEMBER STATES ONLY

Post Title: Senior Technician (Cyber Security)
Grade: NATO Grade G10
Duty location: Paris (Neuilly-sur-Seine), France
Duty start: The position is vacant as of 01 March 2026
Closing Date: 01 April 2026
Vacancy ref.: 260295

The interview of shortlisted candidates is provisionally scheduled to be held in Paris - Neuilly-sur-Seine (FR) mid-May 2026.

1. POST CONTEXT AND RESPONSIBILITIES

- The mission of the NATO STO is to help position the Nations and NATO's S&T investments as a strategic enabler of the knowledge and technical advantage for the defence and security posture of NATO Nations and partner Nations.

- As described in the STO Charter, the STO Collaboration Support Office (CSO) is one of the executive bodies of the STO. Within the framework of the STO Collaborative business model, the CSO provides executive and administrative support to the S&T activities conducted through the STO level 2 committees and level 3 working groups.

- In its areas of expertise, the CSO provides assistance and support to the S&T Board, its Chairperson, the Chief Scientist, and his/her office.

- The Senior Technician (Cyber Security) is an essential member of the CSO CIS Support Branch. The primary duties of the incumbent consist of, often working autonomously, ensuring that effective Cyber Security systems, services and procedures are developed, implemented and adhered to. He/she has a continuous working relationship with CIS Branch staff and external Cyber Security and IT contractors, including NCIA and other Service Providers.

Functions include:

- Contributing to system and service vulnerability threat analysis on new and updated systems and services, and applying necessary safeguards in order to minimize risk.

- Investigating security incidents, either independently or in conjunction with the Principal Technician (Cyber Security) and/or NATO Cyber Security Center and taking appropriate action.

- Monitoring all cyber security services and applications for signs of intrusion, anomalies and potential cyberattack or threat.

- Investigating by data gathering individual anomalies and/or attacks, and contributing to prioritization by severity.

- Contributing to the development, administration, and improvement of Security Information and Event Management (SIEM) solutions, to include; dedicated dash board creation and monitoring to target specific anomalies, patch and update implementation, tailoring to encompass all existing and new security systems and services, data correlation and log management.

- Creating and implementing rules to combat identified threats.

- Applying and functional testing all security related system and service patches and updates in a timely manner.

- Administering all network security devices and services.

- Contributing to the identification of security issues and concerns.

- Working closely with internal (e.g. IKM office, OCO staff) and/or external cybersecurity actors (e.g. ICT contractors or service providers, including NCIA, SHAPE J2, or other NATO body);

- Designing and implementing evolution of the network security architecture and additional SIEM.

- Ensuring security procedures are adhered to, for example, mobile device usage etc.

- Collaborating with CIS Support Technicians, administering the CIS virtual infrastructure. Installation and configuration including policy, security, antivirus, backup and storage solutions.

- Analyzing and resolving level 2 Cyber Security related incident tickets for the CSO and STO community, escalating level 3 incident tickets or issues to as required.

- Investigate and resolving issues in a systematic approach with the help of NCI Agency and/or external Cyber Security and IT contractors when necessary.

- Participating in the development and maintenance of suitable disaster recovery plan.

- Interacting with CSO, STO and other NATO bodies, to include; providing Cyber Security guidance and subject matter expertise, troubleshooting issues.

- Support implementation, integration, documentation and testing new systems and services using best practice throughout the lifecycle.

- Performing duties of Cryptographic Custodian or alternate.

- Assisting in preparation of, and delivering, Cyber Security related briefings, and presentations.

Special Requirements and Additional Duties

- Performing other related functions as directed by the Branch Head, CIS Support.

- Occasionally executing on-call duty, providing Cybersecurity and COMSEC support outside of working hours, weekends and during national holidays.

- Occasionally travelling abroad in support of the Science and Technology Organization high visibility event.

2. AUTHORITY

- The Senior Technician (Cyber Security) reports to the Branch Head (CIS Support).

3. QUALIFICATIONS

ESSENTIAL

Professional /Experience

a) Broad and sound knowledge and experience in Communication and Information Systems.

b) Detailed knowledge of security system and service administration.

c) Technical knowledge of hacking tools and techniques.

d) Experience in the design and implementation of complex IT network security architectures.

Education/Training

Higher Secondary education and completed advanced vocational training in Cyber Security coupled with a minimum of 3-5 years professional experience working in the field of Cyber Security, to the level of CISSP/CEH or equivalent.

Language

Good knowledge of one of the two NATO official languages (SLP 3322) and fair knowledge of the other (SLP 2222). The work is mainly conducted in English.

DESIRABLE

Professional /Experience

a) Familiar with the NATO Information Security policy.

b) Familiar with the NATO Cyber Security policy.

Education/Training

Recognized certifications in IT security systems and services e.g. CISSP, CEH.

Language

a) Very good knowledge of both NATO official languages.

b) Knowledge of other European language(s).

4. COMPETENCIES

1. *The incumbent must demonstrate the following personal attributes:*

a) Reliable, trustworthy, discreet, with high sense of responsibility, showing tact, diplomacy, courtesy and with a pleasant personality.

b) Good judgment.

c) Willing to take initiative.

d) Capable of working in a demanding scientific environment.

e) Flexible in response to changing requirements.

f) Willing to travel on CSO business as required and to accept occasional prolonged duty, especially at meetings.

2. *Managerial Responsibilities*

The Senior Technician (Cyber Security) may occasionally be required to supervise the work of contractors.

3. *Professional Contacts*

In the execution of his/her duties, the incumbent will:

a) Work closely with external Cyber Security and IT contractors.

b) Attend CSO meetings where CIS services are required.

c) Interact with staff members of other NATO bodies to establish and coordinate requirements.

4. *Contribution to the Objectives*

The security of the CSO CIS is core to the existence of the collaborative environment needed by the contributors to the STO Collaborative Program of Work. Task Groups and STO members use the CSO collaborative tools, relying on the CSO to provide the protection they expect for the information they share. The requirement to provide a secure collaborative environment is part of the functions of the CSO.

5. SECURITY CLEARANCE LEVEL

The applicant must be eligible for a NATO COSMIC TOP Secret security clearance.

6. WORKING ENVIRONMENT

The incumbent will normally operate in an open office environment, with occasional exposure to excessive noise in a Server Room environment. Long working hours and travel abroad are infrequent but expected.

7. EMPLOYMENT TERMS AND CONDITIONS

The position is at grade G10. The starting basic monthly salary will be Euro 5335.54 (2026 salary value, subject to future adjustments in accordance with NAC decisions), exempt from income tax. Specific allowances may apply, depending on personal circumstances of the incumbent.

NATO International Civilian employees benefit 30 days of annual leave, life and medical insurance, and a retirement pension plan; expatriated Staff also benefits an expatriation allowance, educational allowance for dependent children and biennial home leave.

In accordance with the NATO Civilian Personnel Regulations, the successful candidate will be offered a definite duration contract of three years, which may, on conditions, be followed by another contract. If the successful applicant is seconded from the national administration of one of NATO's member States, a 3-year definite duration contract will be offered, which may be renewed for a further period subject to the agreement of the national authority; the maximum period of service in the post as a seconded staff member is six years.

Serving staff will be offered a contract in accordance with the NATO Civilian Personnel Regulations in force at the date of the contract.

The appointment is subject to the receipt by the CSO of a security clearance (provided by the national Authorities of the incumbent) and to the delivery of a certificate of medical fitness by the CSO Medical Advisor.

8. APPLICATION PROCEDURE

Only nationals of the 32 NATO member countries can apply for this position.

Applications must be submitted as follows, as applicable:

- For NATO serving civilian Staff members only: please apply via the internal recruitment portal (for more information, please contact your local Civilian HR Manager).
- For all other applicants: www.nato.int/recruitment

A Selection Panel will evaluate the applications. Applicants who pass the initial screening will be invited to attend an interview with the Selection Panel to be held in Paris - Neuilly-sur-Seine (FR) mid-May 2026.
Candidates will attach a resume, an application letter and educational qualifications certificates to their application.

NATO will not accept any phase of the recruitment and selection prepared, in whole or in part, by means of generative artificial-intelligence (AI) tools, including and without limitation to chatbots, such as Chat Generative Pre-trained Transformer (Chat GPT), or other language generating tools. NATO reserves the right to screen applications to identify the use of such tools. All applications prepared, in whole or in part, by means of such generative or creative AI applications may be rejected without further consideration at NATO's sole discretion, and NATO reserves the right to take further steps in such cases as appropriate.

Due to the large number of potential candidates, telephone or email enquiries cannot be dealt with.

Notes: NATO as employer values diverse backgrounds and perspectives and is committed to recruiting and retaining a diverse and talented workforce. NATO welcomes applications of nationals from all Member States and strongly encourages women to apply. According to the NATO Civilian Personnel Regulations, Staff members are appointed on the condition that they are over 21 and under 60 years of age at the time of taking up their appointment. However, appointment may be offered to candidates of 60 years of age or more provided that the expiry date of the contract is not later than the date at which the candidate attains the age of 65.