SUPREME HEADQUARTERS ALLIED POWERS EUROPE

TALEO Job Number: 260251

Vacancy Number: G15/26

Post Number: OSC CYPX 0141

Job Title: Senior Engineer (Cyberspace Security)

NATO Grade: G17

Basic Monthly Salary (12 x per year): 8.273.12€, tax free

Closing Date: 29 April 2026

POST CONTEXT/POST SUMMARY

POST CONTEXT/POST SUMMARY

Supreme Headquarters Allied Powers Europe (SHAPE) provides an integrated Strategic Effects framework, employing a multi-domain and multi-region focus to create a 360-degree approach, with the flexibility to enable, upon direction, a seamless transition from Baseline Activities and Current Operations (BACO) up to the Maximum Level of Effort (MLE). SHAPE supports SACEUR in fulfilling his terms of reference, as directed by the North Atlantic Council.

The Cyberspace Directorate directs monitors and coordinates all Cyberspace Operations (CO), Electronic Warfare (EW), Electro Magnetic Spectrum (EMS) activity and Communications and Information Systems (CIS) functional area activities and staff functions across ACO.

The J6 Cyberspace Division provides the strategic staff functions for cyberspace aspects within ACO's strategic direction, planning and risk management to support NATO-led operations, initiatives, exercises and activities.

The Cyberspace Strategic Plans and Policy Branch will provide military Subject Matter Expert (SME) advice, strategic direction and oversight of all cyberspace functional area activities across ACO.

The incumbent will be responsible to support all the Cyberspace Security and Risk Management (CSRM) activities within SPP Branch, including supporting the Cryptographic Authority for ACO; co-chairing the Allied Cryptographic Task Force (ACTF); recommending strategy for NATO crypto modernization; providing permanent cryptographic situational awareness and risk assessment; supporting ACOS J6 in the roles of ACO CIS Operational Authority (ACO CISOA) and Cyberspace Risk Owner for the ACO CIS; and providing strategic CIS security risk and issue assessments.

PRINCIPAL DUTIES

The incumbent's duties are:

- 1) Reviews, analyses and/or initiates reports based on the Cyber Situational Awareness data.

- 2) Advises on strategic Cyberspace security risk management to support ACO CISOA;
- 3) Prepares recommendations for utilization of operational/training Cyber Defence operations resources.
- 4) Preparation and dissemination of cyber operations doctrine, strategic plans, orders, and training directives;
- 5) Development of standards, including doctrine, tactics, techniques and procedures, across the Cyberspace domain to enhance interoperability.
- 6) Leads, initiates and recommends Strategy for Cryptographic Modernisation for communication security in NATO.
- 7) Identifies cryptographic options and requirements supporting COMSEC, TRANSEC and all other cryptographic aspects relevant to NATO AOM;
- 8) Provides ACO interface for Cyberspace Security to NATO Bodies including NOS, NPAG, NPMA, NSAB;
- 9) ACO-lead in identifying operational requirements (Operational Requirements Authority) for ACO CIS Security including cryptography;
- 10) Provides guidance to CyOC operational planners regarding strategic Cyber security requirements and limitations;
- 11) Plans for the continuing maturity of the Cyberspace Security and cryptographic capabilities of NATO;
- 12) Ensures coherence of operational requirements between Cyberspace Security related projects and all other Cyberspace related projects;
- 13) Utilizes information and requirements gathered from Policy documents and technical assessments and identifies operational requirements with regard to NATO's AOM mandate;
- 14) Supports ACO strategic initiatives as tasked, including cryptographic modernisation and FMN;
- 15) Committee Participation: Co-Chairs the Alliance Crypto Task Force (ACTF), which reports directly to MC - CaP4 (IA & CD) and subordinate CaTs – contributor as required.
- 16) Committee Participation: Information Security Systems Sub-Commitee - Contributor

SPECIAL REQUIREMENTS AND ADDITIONAL DUTIES

The incumbent may be required to undertake deployments in support of military operations and exercises, and/or TDY assignments, both within and without NATO boundaries up to 180 days. The employee may be required to perform a similar range of duties elsewhere within the organization at the same grade without there being any change to the contract.

The risk of injury is categorised as No risk / risk might increase when deployed.

ESSENTIAL QUALIFICATIONS

a. Professional/Experience

- Minimum 4 years of experience in CIS risk management and cybersecurity in defence, government, or large critical infrastructures.
- Strong knowledge of cybersecurity governance frameworks (risk management, accreditation, security controls, compliance).

- Minimum 4 years of experience of military CIS systems (satcom, tactical radios, data links, radar) and experience supporting system accreditation, security risk assessments, and authority-to-operate processes.

- Good knowledge of NATO CIS security policies and governance within NATO environments.

b. Education/Training

University Degree in engineering, electronics or Communications Electronics, and 4 years function related experience, or Higher Secondary education and completed advanced vocational training leading to a professional qualification or professional accreditation with 7 years post related experience.

c. Language

English - SLP 3333 - (Listening, Speaking, Reading and Writing)

NOTE: The work both oral and written in this post and in this Headquarters as a whole is conducted mainly in English.

DESIRABLE QUALIFICATIONS

a. Professional Experience

- Knowledge on cloud security, cross-domain solutions, and information assurance in classified networks.

- Experience supporting operations, exercises, or mission networks from a cybersecurity perspective.

- Experience in cyber incident management, vulnerability management, or security monitoring in operational environments.

- Broad military background/staff experience at high level HQ including previous experience within NATO structures, commands, or agencies.

b. Education/Training

- Professional cybersecurity certifications such as CISSP, CISM, CISA, or certified in Risk and Information Systems Control (CRISC).

- PRINCE II or Project Management Professional (PMP) or internationally recognized equivalent.

- ITIL version 3 or internationally recognized equivalent.

- COBIT5 or internationally recognized equivalent.

ATTRIBUTES/COMPETENCIES

• Personal Attributes: Self-starter. Analytical and conceptual thinker. Team worker. Must impact/ influence activities within the various stakeholders' organization.

• Professional Contacts: Must have a very good working relationship with Military Committee Agencies such as DACAN and SECAN, the Crypto producing Nations' NCSA, as well as INFOSEC staff within the subordinate Commands.

• Contribution To Objectives: Establishes cryptographic Direction and Guidance for the NATO CIS Group and the subordinate Commands for Alliance Operations and Missions (AOM). Maintains close coordination with the NATO cryptographic community. Develops and maintains cryptographic subject matter expertise relating to Alliance Operations and Missions. Ensures ACO and AOM wide collaboration and compliance on all cryptographic aspects.

REMARKS:

Duration of contract: Serving staff members will be offered a contract according to the NATO Civilian Personnel Regulations (NCPR). Newly recruited staff will be offered a definite duration contract of three years normally followed by an indefinite duration contract.

The salary will be the basic entry-level monthly salary defined by the NATO Grade of the post, which may be augmented by allowances based on the selected staff member's eligibility, and which is subject to the withholding of approximately 20% for pension and medical insurance contributions.

NATO is committed to diversity and inclusion, and strives to provide equal access to employment, advancement, and retention, independent of gender, age, nationality, ethnic origin, religion or belief, cultural background, sexual orientation, and disability. NATO welcomes applications of nationals from all member Nations.

Building integrity is a key element of NATO's core tasks. As an employer, NATO values commitment to the principles of integrity, transparency, and accountability in accordance with international norms and practices established for the defence and related security sector. Selected candidates are expected to be role models of integrity, and to promote good governance through ongoing efforts in their work.

We believe that all people are capable of great things. Because of this, we encourage you to apply even if you do not meet all of the criteria listed within this job description.

Applicants who prove to be competent for the post but who are not successful in this competition may be offered an appointment in another post of a similar nature, which might become vacant in the near future, albeit at the same or lower grade, provided they meet the necessary requirements.

ADDITIONAL INFORMATION

Applications are to be submitted using NATO Talent Acquisition Platform (NTAP) (https://nato.taleo.net/careersection/2/jobsearch.ftl?lang-en). Applications submitted by other means (e.g. mail, e-mail, fax, etc) are not accepted.

More information to be found on these links:

6 Tips for Applying to NATO

Application Process

A copy of the qualification/certificate covering the highest level of education required by the job description must be provided as an attachment. Essential information must be included in the application form. Particular attention should be given to Education and Experience section of the application form. The application should be in English. Shortlisted candidates will be requested to provide original documentary evidence and a set of copies supporting statements in their applications. After submitting your application, you will receive an acknowledgement of receipt of your application.

Remarks:

A) Only nationals from the 32 NATO member states can apply for vacancies at SHAPE.

B) Applications are automatically acknowledged within one working day after submission. In the absence of an acknowledgement please make sure the submission process is completed, or, re-submit the application.

C) Candidates' individual telephone, e-mail or telefax enquiries cannot be dealt with. All candidates will receive an answer indicating the outcome of their application

D) NATO will not accept any recruitment or selection materials created, in whole or in part, using generative artificial-intelligence tools, including but not limited to chatbots such as ChatGPT or other language-generation systems. NATO may screen submissions to detect such use. Any application prepared with generative or creative AI may be rejected at NATO's sole discretion, and further action may be taken as appropriate.