**SUPREME HEADQUARTERS ALLIED POWERS EUROPE**

**TALEO Job Number: 241861**

**Vacancy Number: G193/24**

**Post Number: OCG COAX 0050**

**Job Title: Technician (Information Assurance)**

**NATO Grade: G10**

**Basic Monthly Salary (12 x per year): 4,565.36€, tax free**

**Closing Date: Sunday 20 January 2025**

## POST CONTEXT/POST SUMMARY

The NATO Communications and Information Systems (CIS) Group plans, deliver and supports NATO's Deployable Communication and Information Systems (DCIS) in order to enable command and control (C2) for NATO's deployed HQs.

The J2/6 Division is the technical coordination authority for Deployable Communication Information Systems and is responsible for the operational integration, coordination, direction and provision of required technical services for the NATO Communications Information Systems Group and NATO Signal Battalions.

The Information Assurance and Cyber Defence Branch is the NCISG's coordinating authority for organizational security, Information Assurance (IA), Cyber Defence and Cyberspace Intelligence. It is also responsible for the planning, coordinating, operational integration, monitoring, assessing, and auditing of IA and Cyber Defence activities supporting Deployable Communications Information Systems (DCIS).

The Information Assurance and Security Services Section is responsible for Deployable Communication Information Systems Information Assurance and security engineering, and the enforcement of the NATO security policy throughout NATO Communications Information Systems Group.

The incumbent is responsible for technical support to all IA and Security activities of NCISG.

## PRINCIPAL DUTIES

The incumbent's duties are:

1. Principal technician supporting NATO CIS Group operational Information Assurance.

2. Supports the implementation of computer and network security projects at all sites within the NATO CIS Group AOR.

3. Supports the provision and delivery of Information Assurance and Security Awareness training and presentations to the NATO CIS Group.

4. Supports CIS Risk Management process by identifying risks, making assessments, and formulating recommendations to reduce the risks within computer security and IA functions.

5. Supports computer security and IA by implementing procedures and techniques, analyzing current practices, installing and operating monitoring tools and Security Audit platforms to evaluate overall Group CIS security with minimal supervision.

6. Provides IA assistance to NATO operations and exercises, which includes support to exercise coordination and planning, pre-deployment configuration checks, and exercise participation.

7. Assists in the daily management of the NATO CIS Group Security Accreditations coordinating directly with NCIA and coordinates with the NSBs to validate accreditation packages prior to SAA review.

8. Provides technical support for DCM Security Design and Management.

9. Provides technical support in the areas of: CIS Security measures, Disaster Recovery & Backup, Business Continuity, Risk Management, technical documentation and evaluation of new technologies.

10. Provides support in solving technical issues and the validation of IA requirements.

11. Assists in the coordination of PKI requirements in support of federated NATO operations and exercises.

12. Supports development of best practices and security operating procedures for NCISG HQ and subordinate units.

13. Supports the analysis of security systems and seek improvements on a continuous basis.
14. Participates in risk assessment and incident response activities.

15. Supports validation of security configurations and access to security infrastructure tools, as boundary protection, and endpoint protection systems.

16. Provides technical support for NSB s and DCMs Security Design and Management.

17. Provides support in solving technical issues and the validation of IA requirements.

18. Works with Information Security Team to research and recommend security enhancements to NCISG management.

19. Provides Support for NCISG Cyber Hygiene programme, and implementation of DCIS security controls.

20. Provide support for Cyber Intelligence and Threat assessments.

21. Supports information security policies, procedures, standards and guidelines.

22. Stay current on IT security technologies, trends and news.

23. Provides direct support to NCISG staff for security related issues.

## SPECIAL REQUIREMENTS AND ADDITIONAL DUTIES

1. 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.

## ESSENTIAL QUALIFICATIONS

### A. Professional/Experience

Experience

- Experience in ADP related posts.

- Knowledge of TCP/IP stacks protocols and ports.

- Practical experience in network security audit, analysis, and architecture.

- Practical experience in security incidents handling and response

- Practical experience in risk-based security assessments and audits.

- Work experience in computer security tools and vulnerability assessment methodologies.

- Comprehensive knowledge of the principles of computer and communications security, networking, and the vulnerabilities of modern operating systems and applications.

- Minimum 2 years of experience providing IA and security services support.

- Completed ITIL V3/V4 Foundation Certification.

### B. Education/Training

Higher Secondary education and intermediate vocational training in information security, computer science or related discipline which might lead to a formal qualification with 3 years' experience, or Secondary education and completed advanced vocational training in that discipline leading to a professional qualification or professional accreditation with 4 years post related experience.

### C. Language

English - SLP 3322 - (Listening, Speaking, Reading and Writing)

## DESIRABLE QUALIFICATIONS

### A. Professional Experience

1. Information systems security audit.
2. Information systems engineering and maintenance; INFOSEC implementation; computer security knowledge of CIS and its concepts, policies and architectures.
3. Information systems security audit.
4. Information systems engineering and maintenance; INFOSEC implementation; computer security knowledge of CIS and its concepts, policies and architectures.
5. Experience in COMSEC/Crypto positions
6. Implementation of IA policies and procedures.
7. Professional certifications in IA.
8. Security configuration of Microsoft Windows Server current approved version.
9. Usage of Microsoft Visio.
10. Usage of Risk Assessment and Management tools.

### B. Education/Training

1. CIS Security Professional Certifications or Studies
2. Post graduate diplomas in cyber Security/cyber Defence
3. NATO Security Course (MPG-MP-2699) provided by NATO - School Oberammergau (NSO)
4. NATO CIS security and/or COMSEC Crypto courses provided by NATO Communications and Information Academy (NCI Academy)
5. NATO CIS Security Officer/ Infosec courses provided by NATO Communications and Information Academy (NCI Academy)

## ATTRIBUTES/COMPETENCIES

• Personal Attributes:

1. Possess excellent knowledge and advanced thinking in IT/computer security and a deep understanding of NATO Consultation, Command and Control objectives and goals as well as operational requirements in support of NATO Command and Control Information Systems, particularly as they relate to security.

2. Actively assumes direct responsibility for a broad spectrum of management and support tasks.

3. Self-starts required activities based on creative thinking and conceptual foresight, is sensitive to the emergence of problems, and demonstrates sound independent judgement.

4. Works without direct supervision and maintains a high level of performance under pressure.

5. Able to propose effective and efficient courses of action after thorough analysis of complex information.

6. Possess excellent communication skills.

• Professional Contacts: Regular professional contacts with others inside and/or outside immediate organisation on functional matters. Solicits/gives information and provides advice/guidance.

• Contribution to Objectives: Work involves the provision of information or analysis of part of a task assisting others to take action within the organisation.

**REMARKS:**

During crisis of MLE the incumbent is reassigned to the NCISG HQ Crisis Establishment (CE) or the DCIS Support Group, as detailed in the respective CE.

**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 5 NTAP allows adding attachments.
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

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.

**HOW TO APPLY FOR A NATO CIVILIAN POST AT SHAPE:**

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

Shortlisted candidates will be requested to provide original documentary evidence and a set of copies supporting statements in their applications. Appointment is subject to obtaining a NS security clearance and a medical certificate.