

**SUPREME HEADQUARTERS ALLIED POWERS EUROPE**

Vacancy Number: G122/26

TALEO Number: 21165

Job Title: Staff Assistant (Cyber Security/CIS Security Accreditation)

Post Location: Casteau/Mons, 60 Km south of Brussels (Belgium)

Grade: G11

Basic Monthly Salary: 5,234.63 EUR

Closing Date: Tuesday 28 July 2026

1. POST CONTEXT

SHAPE is NATO's strategic headquarters, supporting SACEUR and ensuring the Alliance can respond effectively to crises and operations. Within SHAPE, the Strategic Employment Directorate provides situational awareness and assessments that help NATO understand emerging issues and coordinate responses.

The role supports the ACO Security Accreditation Authority (SAA) by helping to accredit CIS systems and projects—especially those linked to NATO's Digital Backbone and technology transformation. This includes working with project teams to gather cyber requirements, guide them through the accreditation process, and ensure systems remain secure throughout their lifecycle.

2. PRINCIPAL DUTIES

The incumbent's duties are:

- 1) Support the ACO SAA for the security accreditation of all relevant CIS projects and systems, in scope of Digital Backbone and technology transformation, supporting project staffs and system management groups on collection of CIS cyber requirements and accreditation matters throughout the CIS life-cycle.
- 2) Under direction and guidance of CIS Security Supervisor Information Assurance Inspector, provide accreditation for enormous amount of newly identified CIS

- 3) On behalf of ACO SAA support and execute security audits of CIS and contribute to security inspections, support improvements and developments of CIS to meet NATO security requirements and standards.
- 4) Maintain working level staff liaison with NATO CIS Operational Authorities on Accreditation matters including Risk Management under umbrella of Cyber Risk Management Group (CRMG).
- 5) Support collection of requirements and implementation of new accreditation tools.
- 6) Support Section staff officer's duties in accreditation efforts of NATO CIS with a special attention to Maritime CIS and advance consultation Networks
- 7) Support to the Section staff officer's duties in the evaluation / assessment of Information Assurance (IA) threat vectors and IA Risk Assessments as well as evaluate systems' test results and vulnerability assessment reports.
- 8) Attend meetings / events in regards to CIS Security and Information Assurance on behalf of the section.
- 9) Support workshops, training events and exercises, as required.

3. 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.

4. ESSENTIAL QUALIFICATIONS

1. Professional/Experience

- 1) Experience in information security
- 2) Experience conducting assessments of network security tools, firewalls and internet security, sustainability, real-time systems, application design, and/or asset management.

2. Education/Training

University Degree in information security, computer science, audit, mathematics, statistics, business administration or related discipline and 1 year post-related experience, or Higher Secondary education and completed advanced vocational training in that discipline leading to a professional qualification or professional accreditation and 2 years of post-related experience.

In case of ambiguity the required job specific experience have priority over the standard education and training levels and experience described here.

3. Language

English – SPL 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.

5. DESIRABLE QUALIFICATIONS

1. Professional/Experience

- 1) Experience as a CIS Security Engineer
- 2) Specialist either in CIS or in Security and cross-trained in INFOSEC;
- 3) Background in military security work covering all aspects of physical security, document security, personnel security, and information assurance

6. COMPETENCIES

- 1) Personal Attributes: - The incumbent must have an outstanding task management and communication skills.
 - a. He/she must be innovative and possess the intellectual ability to create, advertise and instruct CIS Security programmes that not only meet NATO security policy requirements but are pragmatic from operational perspective and implementable at the lowest command levels.
 - b. Tact, judgment, adaptability, coupled with motivational and listening skills. A sense of diplomacy and propriety in order to work harmoniously with colleagues and other staff, both civilian and military.
 - c. Able to work effectively to support the team activities.
 - d. Willingness to adapt to new and evolving processes and organizational structures.
- 2) Professional Contacts: This post requires to establish and maintain constant stakeholder management. The incumbent will be required to maintain established staff level network and to contribute to the CIS Security Accreditation process.
- 3) Contribution to Objectives: The incumbent supports the CIS Security Accreditation process through technical assessments, advice and information/task management. The ACO Security accreditation process is executed on behalf of SACEUR and crucial for the support of ACOS

J2 as the principal security advisor of ACO, it forms the last line of defence in regards to the analysis of operational requirements, which are translated into technical specifications and then matched and compared to current CIS Security policy and guidance documents. The incumbent is also responsible for supporting NATO / ACO Security accreditation tools and portals (or changes to them), based on the requirements coming out of ACO.

7.CONTRACT

The successful candidate will fill this post as a Project Related NATO International Civilian (PLN) with a **15 month definite duration contract** within the NATO 2030 Agenda. On expiry of this term the PLN will be deleted or absorbed into the ceiling pending approval or will exceptionally be considered for extension.

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.

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 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
- E) As part of the recruitment process, the organization may review publicly available information to assess potential conflicts of interest, reputational risks, or behaviors inconsistent with the organization's values.