NOTIFICATION OF A CIVILIAN PERSONNEL REQUIREMENT
AT JOINT FORCE COMMAND BRUNSSUM HEADQUARTERS

Our Requirement:
Title: Staff Officer (Communications and Information Systems (CIS) Security)
Grade: 15
Duty Location: Brunssum, The Netherlands
Requirement filling date: as soon as possible
Closing date for applications: 10 May 2026

Our organisation
Joint Force Command Brunssum (JFCBS) provides a Joint headquarters to plan, prepare and conduct operations to support NATO's core tasks, at the Joint Operational level, as directed by Supreme Allied Commander Europe (SACEUR). The Operations Directorate is responsible for directing, monitoring, coordinating and assessing operational functions and advising the Chief of Staff (COS) regarding all regionally focused operational activities. The J2 Division provides Intelligence in support of the planning, preparation, conduct and assessment of NATO assigned operations. The Joint Intelligence Operations Branch provides intelligence support to the overall Joint Targeting effort in JFCBS and ensures intelligence contribution to situational awareness / understanding (SA/SU), feeding to the Allied Command Operations (ACO) wide database. The incumbent is responsible for CIS Security and Security issues and is a member of the Inspection team, within the J2X Section of the J2/6X Intelligence Security, Systems & Support Branch.

The main duties of Staff Officer (CIS Security) are to:
- Develop, implement and enforce CIS Security and Security policies, directives and guidelines in peacetime and operations.
- Contribute to the Coordination of all CIS requirements within JFCBS HQ.
- Coordinate all CIS Security issues within the JFCBS HQ and with other national/NATO agencies, commands and organisations.
- Inspect subordinate Headquarters (HQs) and ensure compliance with NATO CIS and Security policies.
- Undertake work as part of a project team or working group as directed or assigned.
- Prepare/assist in the preparation of meetings, agendas, programs, minutes.
- Provide advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards.
- Obtain and act on vulnerability information and conduct security risk assessments, business impact analysis and accreditation on complex information systems.
- Investigate major breaches of CIS security and recommend appropriate control improvements. Contribute to development of information security policy, standards and guidelines.

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. Such operational deployment may exceed 30 days duration up to 183 days in any period of 547 days and may be on short notice. For NATO International Civilian Staff, acceptance of an employment contract linked to this post constitutes agreement to deploy in excess of 30 days if required.

Required Qualifications are:

- English – good – NATO Standard Language Proficiency 3333
  (Listening, Speaking, Reading and Writing) in accordance with NATO standard agreement (STANAG) 6001.
  NOTE: The work both oral and written in this post and in this Headquarters as a whole is conducted mainly in English.
- University Degree or equivalent in related field/discipline
  (equivalent is Higher Secondary Education AND completed advanced vocational training in relevant field leading to a professional certification or accreditation).
- Proven knowledge of computer and security principles, networking and operating system vulnerabilities and incident handling.
- Minimum 4 years' professional experience with CIS/network security.
- Minimum 2 years' experience applying Security policy preferably in CIS.
- Minimum 2 years' experience in the selection, design, justification, implementation and operation of Security controls and management strategies.

Desirable Qualifications are:

- Experience performing joint staff functions, preferably in a NATO environment.
- Participation in National or NATO CIS and/or security related trainings and exercises.
- Experience in Information Technology (IT) - governance.
- Completion of relevant training/courses obtaining certifications such as Certified Information Systems Security Professional (CISSP) – Certified Information Security Manager (CISM) – Certified Information Systems Auditor (CISA) – International Organization for Standardization / International Electrotechnical Commission (ISO/IEC 27001), Global Information Assurance Certification (GIAC).

The successful candidate possesses following personal attributes:

- ✓ Excellent communication skills, both oral and written - able to communicate at all levels;
- ✓ High level of interpersonal skills including tact and diplomacy;
- ✓ Ability to take initiative;
- ✓ Ability to work with external stakeholders.

The selected candidate must be able to obtain and maintain a security clearance and is required to pass a medical examination before an employment contract offer will be released. The medical examination will take place with our medical consultant, it is required to determine if the recommended candidate is fit to perform the duties and is deployable to NATO's areas of operation.

Due date for receipt of applications: Sunday 10 May 2026: 23:59.

Candidates have to apply electronically in NATO Talent Acquisition Program:
https://nato.taleo.net/careersection/2/jobsearch.ftl?lang=en

IMPORTANT:
Please be aware that a Selection Board will only assess the information provided in the job submission form including the answers to the pre-screening questions and description of your work experiences. Your answers must be comprehensive and stand alone; do not rely on attached documents for essential information *(Attachments are supporting documents and should not be referred to in the job submission).* For example, if a pre-selection question asks you to justify how you meet the minimum experience requirement, you must explicitly detail in the answer box *how* your experience directly aligns with, or exceeds, the stated requirement. Simply stating you meet the requirement is insufficient; provide concrete examples and quantifiable details. These experiences should also be included in the description of your work experiences.

Only candidates meeting ALL essential required qualifications will be considered and be assessed in competition with other candidates.
Please note that 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