HQ SACT VACANCY NOTICE 240222

Applications are now invited for the post of Crypto SME, TSC FCVX 0170, NATO Grade (NG) 17 on the staff of the Supreme Headquarters Allied Commander Transformation (SACT), a NATO Strategic Command in Norfolk, Virginia, USA.

Applications must be made on line:
https://nato.taleo.net/careersection/2/jobsearch.ftl?lang=en

Closing date for applications: 6 March 2024

Location: Headquarters Supreme Allied Commander Transformation (HQ SACT), Norfolk, VA, USA

- **Notes for candidates:** the candidature of NATO redundant staff at grade A3/NG17 will be considered before any other candidates.

- **Notes for NATO Civilian Human Resources Managers:** If you have qualified redundant staff at grade A3/NG17, please advise the HQ SACT Civilian HR Manager no later than the closing date.

Contract: Serving NATO International Civilian staff will be offered a contract in accordance with the NATO Civilian Personnel Regulations. Newly recruited staff will be offered a three year definite duration contract.

Salary: Starting basic salary is USD 10,090.40 per month to which relevant allowances will be added.

For any queries, please contact the HQ SACT Recruitment Team at civilianpersonnel@act.nato.int

Crypto SME - TSC FCVX 0170

Are you a Cryptographic specialist? If so, this position offers you a unique opportunity to support the NATO Alliance at its Capability Development Command.

Post Context

ACT contributes to preserving the peace, security and territorial integrity of Alliance member states by leading, at Strategic Command level, Warfare Development required to enhance NATO's posture, military structures, forces, capabilities and doctrines.

The Capability Development Directorate (CAPDEV) comprises two Divisions—Requirements and Capabilities. The Directorate supports SACT in his Capabilities Requirement Authority (CRA) role. It is responsible for a holistic through lifecycle Capability Development approach that infuses innovation and transformative efforts that are an integral part of the Warfare Development. This includes responsibilities for elicitation, development, capture and collection, quality review, traceability and visibility of capability requirements.

The Capabilities Division coordinates the development of capabilities from capability planning through acceptance and then disposal with the management entities, NATO Headquarters staff and the NATO Governance Structure. This entails synchronizing horizontally across capabilities to achieve coherent efforts and outcomes.

The Cyberspace Branch provides scientific, technical and operational expertise for the development and continuous improvement of modern and agile Cyberspace capabilities including Cyber Defence and enabling cryptographic infrastructure. The Branch provides services and products through a competency-aligned structure to support appropriate product, programme coordination across DOTMLPFI lines of development throughout the lifecycle. The Branch supports cyber concepts development, capability requirements elicitation, architectures (including cryptographic reference and target architectures) and federated interoperability. This includes leveraging applied science, technology, operations research and horizon scanning. The Branch leads the development of Capability Programme Plans (CPPs) and ensures delivery of programme outcomes by assessing throughout the lifecycle the CSSPR against agreed tolerances. The Branch leads the acceptance testing and documentation of assigned capabilities. The Branch analyses emerging technologies with stakeholders. It ensures military and technical coherence and persistent interoperability.

He/she serves as the Cryptographic Engineer (Subject Matter Expert, SME) of the Cyberspace Capabilities Section within the Cyberspace Branch and provides support to both Warfare Development and Capability Development within the Branch.

Reports to: Section Head (Programme Director Cyberspace Caps)

Principal Duties: His/her duties are:

a. Provide expertise on cryptographic principle, theories, designs, systems, devices and their implementation and operation to ACT and especially to the Cyberspace Branch.

b. Contribute, under the guidance of Programme Director (PD) Cyberspace Capabilities, to the development of NATO common funded cyber Capabilities.

c. Support, as required, the development and submission of stand-alone cryptographic projects and Urgent Requirement Requests (URRs).

d. Participate and support the Allied Cryptographic Task Force (ACTF) and the Crypto Capability Area Team (Crypto CAT), among other NATO cryptographic focused organizations contribute to the development of non-cyber Capabilities by providing crypto specific expertise.

e. Support elicitation of cryptographic requirements and development of associate capabilities.

f. Support the development of cryptography concepts.

h. Interact, if required, with other SME's to provide support of EDT (Emergent and Disruptive Technologies), especially in the field of quantum.

g. Assists the Portfolio Manager, Programme Monitor, Programme Director, and Project Coordinators in the engagement with governance, management and users entities, related with the capability or specific project architectures.

h. Collaborate and liaise with industry, academia, NATO, non-NATO and national partners, in order to, amongst other things, constantly maintain a state-of-the-art picture of emerging architectural analysis and design methodologies.

j. Coordinate engineering and technical requirements with the NATO Communications and Information Agency (NCIA) as the NATO CIS implementation authority.

k. Support HQ SACT Office of Security in process of accreditation of NATO-wide cryptographic projects.

l. Liaise with other ACT Branches, as required.

m. As required, may be assigned as Project Coordinator for projects within the scope of the duties of the post.

Essential Qualifications

1. University Degree in Information technology, computer science, computer networking and communications. or related discipline and 4 years post related experience, or Higher Secondary education and completed advanced vocational training in that discipline leading to a professional qualification or professional accreditation with 5 years post related and 2 years function related experience.

2. Two-three years' previous work experience in the field of applied cryptography, preferably in a project development/oversight role.

3. At least two years working knowledge of cyber security and its application in a complex system of systems environment.

4. Demonstrable applied experience with cryptography, including architectural design, working with and evolving legacy systems and understanding key challenges / opportunities such as the use of Quantum.

5. Experience of working within large projects and providing ongoing support and expertise through an entire project lifecycle, from inception to decommissioning.

6. Ability to clearly communicate highly technical ideas, via both written and verbal mechanisms, and demonstrate strong organizational and planning skills.

Language

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

Desirable Qualifications

a. Professional Experience

1. General knowledge of the organization and structure of NATO.

2. Experience with the NATO Architectural Framework (NAF).

3. Project management certification and / or experience.

4. Demonstrable understanding of Cyberspace operations.

b. Education/Training

1. A Master's level's Degree in Engineering, Mathematics or Computer Science from an accredited university

2. Cyber Defence at Operation Level Course (COP-CD-31954) provided by Cooperative Cyber Defence COE (CCD COE)

3. NATO Staff Officer Orientation Course (ETE-IT-3834) provided by NATO - School Oberammergau (NSO)

Attributes/Competencies

• Personal Attributes: He/she requires the ability to prepare, organize and conduct engagements with all type of stakeholders, from industry to high rank flag officers, of all sizes. This will require excellent communication skills, along with a sense of protocol or etiquette. The above should be complemented with a strong technical background to enable him/her to authoritatively provide and organize contents for the engagement events, while being capable of dealing with potential courses of the

technical discussions. This will require analytical skills and a basic ability to exercise lateral thinking.

He/she will work with a scientifically diverse team of highly technical experts, staff officers, industry staff of all levels and flag level officers and equivalent civilian posts. He/she needs to understand the needs of engagements with those communities and satisfy them through interaction with his/her branch leaders and external stakeholders. An analytical mind able to absorb, comprehend and synthetize heterogeneous inputs is essential.

• Professional Contacts: He/she acts as the cyberspace federation and partnership responsible for the planning and organization of all related engagements. He/she will be required to maintain professional contacts at a reasonable senior level (up to flag officer and civilian equivalent) with stakeholders both within and outside of the HQ. He/she will be the main face interfacing with those contacts towards the organization of working groups, workshops, conferences and other events, and requires a sensible level of formal and professional courtesy, persuasion, and discussion and negotiation abilities.

He/she will have some professional contacts/relations to academia, industry as well as other technicians within NATO. There are no representation duties.

• Contribution To Objectives: He/she actions and performance will to a certain degree determine how internal and external stakeholders engage with the cyber branch objectives and results, which in turn contribute directly to the perception of the HQ ability to perform, as well as the achievement of HQ objectives that require stakeholders support.

He/she will support the development of new cryptographic assets requires one SME.

• Supervisory Responsibilities: Although he/she is not expected to directly manage any HQ staff, he/she will be required to organize teams and their work and activities, being able to influence the work strategy and the expected results. Ability to plan, coordinate and synchronize activities will be required with a varied type of internal and external stakeholders. Soft skills will be essential.

Security Clearance

The successful applicant will be required to apply for and receive a NATO Secret Security Clearance prior to final confirmation of contract and commencement of employment.

Work Environment

He/she will be required to work in a normal office environment.

Contract

Serving NATO International Civilian staff will be offered a contract in accordance with the NATO Civilian Personnel Regulations. Newly recruited staff will be offered a three year definite duration contract.

Notes for Candidates

The HQ SACT web site gives full details on the eligibility criteria and application processes to be adopted by all candidates. However, candidates should particularly note:

- When completing the application form using NATO Talent Acquisition Platform, you are able to add attachments. Only attachments specifically asked for as part of the application process will be considered. All applications **must include** an uploaded a copy of the qualification/certificate covering the highest level of education required by the job description. If this certificate is not in one of the official NATO languages, you should include a translation into English or French. If you are unable to upload this certificate, you must provide an explanation as to why this is the case in your application, for example, "I am deployed and my certificates are in storage".
- Please answer each of the pre-screening questions completely in English. Expressions such as: "please see attached CV, please see annex, please see enclosed document, etc" are not acceptable; this is a cause of immediate rejection of the application.
- Particular attention should be given to Education and Experience section of your application form, which should be populated with details of your career to date and educational achievements and certifications as they relate to your application.

The HQ SACT web site gives details on the eligibility criteria and application processes to be adopted by all candidates.

The candidature of NATO redundant staff at grade A3/NG17 will be considered with priority.

Applicants who are not successful in this competition may be offered an appointment to another post of a similar nature, albeit at the same or a lower grade, provided they meet the necessary requirements.

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.

This vacancy will close on 6 March 2024 @ 17:59hrs (Eastern)/11:59hrs (CET).

Notes for NATO Civilian Human Resources Managers

If you have qualified redundant staff at grade A-3/NG 17, please advise the HQ SACT Civilian HR Manager no later than the closing date.

For any queries, please contact the HQ SACT Recruitment Team at civilianpersonnel@act.nato.int