Applications are now invited for the post of Crypto Subject Matter Expert - 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: 10 October 2022

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

- **Notes for candidates:** the candidature of NATO redundant staff at grade A 3/NG-17 will be considered before any other candidates.

- **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.

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 9421.48 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 Subject Matter Expert - TSC FCVX 0170

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

Schedule: Full-time

Basic Salary: 9421.48 USD per month.

Grade: NG 17

HQ SACT vacancy notice 220694

Are you a senior cryptographic engineer with broad experience working in and leading project teams? If so, this position offers you a unique opportunity to support the NATO Alliance at its Capability Development Directorate, Cyberspace branch.

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.

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 Cyberspace Capability Programme Plans (CPPs) and ensures delivery of programme outcomes by assessing, throughout the lifecycle, the progress of implementation projects 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:** He/she will:

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 crypto Capability Program Plans (CPP).

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.

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

h. Assist 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.

i. 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**

a. University Degree in Engineering, Mathematics or Computer Science from an accredited university

b. 2-3 years’ previous work experience in the field of applied cryptography, preferably in a project development/oversight role.

c. At least 2 years working knowledge of cyber security and its application in a complex system of systems environment.

d. 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.

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

f. 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.
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 in line with a university degree in international relations or similar discipline. 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: His/her 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 the incumbent 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.

There are no reporting responsibilities.

**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 candidature of NATO redundant staff at grade A-3/NG 17 will be considered with priority.

**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