DISCLAIMER: Please note this Project Linked NATO (PLN) International Civilian Agenda 2030 post is pending Budget Committee's approval.

TITLE: PLN Agenda 2030 Staff Officer (Information Security and Cyber Defence)

GRADE: G-17 (A-3)

DIVISION: J6 Cyberspace

DIRECTORATE: SUPPORT

SECURITY CLEARANCE: COSMIC TOP S E C R E T

EMPLOYMENT CONTRACT: 3-year definite duration contract

1. Post Context/Post Summary

Headquarters Allied Joint Force Command Naples is a Joint Headquarters, operating at the Operational Level, capable of executing effective command and control over assigned forces in order to achieve Operational effects in an assigned Joint Operating Area. As a Joint Force Command the relationships with other NATO Command Structure and NATO Force Structure Component Command Headquarters will change between baseline activities, crisis and conflict. It also provides Joint competencies to assigned NATO Force Structure Headquarters tasked to deploy as Joint Task Force Headquarters

The Support Directorate is responsible for planning, directing, monitoring, assessing and coordinating support staff functions.

The J6 Cyberspace Division is responsible for developing plans, policy, and procedures for Communication & Information Systems (CIS) support of JF HQ missions in static, deployable or in deployed operations.

The Cyber Branch will directly align all functional Cyber activities under the Communication & Information Systems (CIS) division and will ensure top to bottom approach providing a roust CIS support relationship between the strategic and operational level HQs.

The incumbent's duties are to provide support and to contribute to planning and execution of DCO, mitigate Cyber incidents; to contribute to implement and maintain required Cyber security and resilience level for NATO CIS Infrastructure (Accreditation, vulnerability and penetration testing, inspections etc.), providing Cyber defense expertise to peacetime vigilance, missions and exercises.

2. Principal Duties

The incumbent's duties are:

- Provide support and contribute to planning and execution of DCO;

- Meet requirements of Cyber Defense Posture and changes;

- Contribute to implement and maintain required Cyber security and resilience level for NATO CIS Infrastructure (Accreditation, vulnerability and penetration testing, inspections etc.)

- Provide Cyber defense expertise to peacetime vigilance, missions and exercises

- Provide Cyberspace related Mobile Training Teams (MTT)

- Create Cyber Security Awareness among users

- Support and contribute to planning and execution of OCO and related SCEPVA process;

- As Functional Coordination Elements DOA Section will represent as J6 Cyberspace in the Functional Integration Elements (i.e. Command and Control (C2), Targeting, Intelligence, Information, Resources, Force protection, CIMIC, etc…)

- Liaises with local CIS Service Provider regards Cybersecurity activities.

- Assists CIS SECURITY/Cyber Defense/Intel policies, directives and guidelines in peacetime and Operations.

- Assists CIS SECURITY and Cyber Defense/Intel programme coordination within the HQ.

- Assists all CIS SECURITY requirements within JF HQ AOR.

- Assists all CIS SECURITY and Cyber Defense/Intel within JF HQ and with other national/NATO agencies, commands and organisations.

- Assists with Inspections of subordinate HQs and ensures compliance with NATO CIS Security policies.

- Core member of the Cyber Defense Working Group and Cyber Cell.

- Assists conducting co-ordination for any cyber crisis and for cyber defense for ongoing operations.

- Utilize cyber intelligence products to support ongoing operations.

- Undertakes work as part of a project team or working group as directed or assigned.

- Ensure communication and information systems (CIS), including networks and data repositories highly resilient to threats from cyberspace both in peacetime and during armed conflict.

- Conduct defensive actions in or through cyberspace to preserve friendly freedom of action and force protection in cyberspace.

- Contribute to the mission assurance process by protecting or ensuring the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information system, infrastructure, and supply chains, critical to the execution of NATO mission-essential functions in any operating environment or condition.

- Beware of adversaries' capabilities to launch cyberspace operations against own forces and, therefore, plan to respond them as appropriate.

3. Special Requirements and Additional Duties

The employee may be required to perform a similar range of duties elsewhere within the organisation at the same grade without there being any change to the contract

Depending on requirements, may be required to direct and supervise the work priorities of one or more HQ multifunctional teams. The work is normally performed in a Normal NATO office working environment.

Normal Working Conditions apply. The risk of injury is categorised as No Risk.

4. Essential Qualifications

a. Education and Professional Experience

University Degree in information security, computer science 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.

Experience working within Information security

Experience developing and communicating corporate information security policy, standards and guidelines.

c. Language

English - SLP 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

a. Professional Experience

Background experience covering Joint staff functions, preferably in a NATO environment.

- Experience in Security Management and Information Security.

- Knowledge of the Intelligence cycle, processes and J6Cy, J3 and J2 functional activities.

b. Training

• NATO Open Source Intelligence Course (INT-AS-3859) provided by NATO - School Oberammergau (NSO)

• (Inactive) Cyber Defence NATO CIS Security Officer (INFOSEC Version 2.0) (CCC-ET-32256) provided by NATO - Communications and Information Systems School (NCISS)

• (Inactive) Comprehensive Operational Level Planning Course (JPL-OP-22005) provided by PTEC - Crisis Management and Multinational Operations Department (CMMOD)

• (Inactive) NATO Information Operations Course (STC-IO-2536) provided by NATO - School Oberammergau (NSO)

• Network Security Course (COP-CD-31369) provided by NATO - School Oberammergau (NSO)

c. Language

English: SLP 4343

6. Attributes/Competencies

• Personal Attributes: The incumbent works under little or no supervision. Uses independent judgement to propose solutions based on resources available. Incumbent must poses maturity, poise, good communication skills, persuasion as well as tact. The incumbent is technological inclined and instinctively curios keeping abreast of latest technological advancements.

• Professional Contacts: The incumbent will be required to discuss and/or negotiate with individuals from other organizations to share ideas and find solutions to common problems.

• Contribution To Objectives: The incumbent, contributes to higher level of DCO and OCO, feeds the Situation Awareness (CySA) for the HQ, and provides Direction and Guidance to the subordinate Commands.

There are no reporting responsibilities.

This post reports to: OJS RCCX 0010 - Branch Head (Cyber Defence) - OF-5

This post does not deputises anybody. This post is not deputised by anybody.

CONTRACT

The successful candidate will be offered a 3-year definite duration contract within the NATO Agenda 2030. The basic entry-level monthly salary for a NATO Grade 17 (A-3) in Italy is Euro 7,319.21 which is exempt from national taxation, and which may be augmented based on the selected candidate's personal status.

INSTRUCTIONS TO APPLY:

HQ JFC Naples uses NATO Talent Acquisition Platform. In order to apply for this vacancy, please visit the platform at: https://nato.taleo.net/careersection/2/jobsearch.ftl?lang=en, and search for vacancies within HQ JFC Naples with duty location Naples, Italy.

Please attach relevant certificates to the application. Note that once you create your profile, you will be able to use it to apply for other vacancies within NATO.

Please note:

Staff members are appointed to and hold posts on the establishment of a NATO body only on condition that:

- They are nationals of a NATO member country

- They are over 21 and under 60 years of age at the time of taking up their appointments. Appointments of definite duration may be offered to candidates of 60 years of age or more, provided that the expiry date of the contract is not later than the date at which the candidate attains the age of 65.

ADDITIONAL INFORMATION:

A NATO security clearance and approval of the candidate's medical file by the NATO Medical Advisor are essential conditions for appointment to this post. Applicants are not required to possess a clearance at the time of applying, but they must be eligible for a clearance. HQ JFC Naples will take action to obtain the required security clearance from the successful candidates' national authorities.

The selected candidate will be affiliated to the NATO Defined Contribution Pension Scheme (DCPS) system. For information, please visit https://www.nato.int/cps/en/natolive/86790.ht