POST NO. **ODS MCMX 0040**

DIVISION: **Communications and Information Systems Platoon**
TITLE: **Technician (Cyber Defence)**
GRADE: G-10
Directorate Maintenance and Support Company

Division Communications and Information Systems Platoon

1. POST CONTEXT

NATO Signal Battalion operates, maintains, and sustains Deployable Communication Information Systems (DCIS) to enable command and control (C2) in support of deployed NATO Headquarters and entities during Alliance operations, missions and exercises.

The Maintenance and Support Company (M&S Coy) is responsible for Level 1 and Level 2 CIS support of NATO DCIS and for Level 1 and Level 2 preventive and corrective maintenance of non-CIS equipment.

The Communications and Information Systems Platoon is responsible for Communications and Information Systems (CIS) Level 2/2+ CIS support of all CIS assets integral to the Battalion.

The Mobile Communications, Information Systems and Cyber Defence Section (CIS) is responsible for maintaining and repairing cyber protection systems in support of NSB information system functions.

The incumbent is responsible for the protection of classified/unclassified NATO Deployed CIS (DCIS) from Cyberspace threats.

2. Principal Duties

The incumbent's duties are:

1. Identifying system vulnerabilities and possible threats and then applying the necessary safeguards (both technical and administrative) to minimize those vulnerabilities and defend against potential attacks.

2. Performing routine system and network monitoring and detecting security incidents or bad security practices that may lead to system compromise.

3. Mentoring and providing on-the-job training to the military Cyber Defence technicians of the M&S Coy Mob CIS and Cyber Defence section.

4. Providing mentoring and technical guidance to the NSB DCMs IS technicians for vulnerability resolution and mitigation.

5. Supporting and guiding the daily Cyber hygiene duties and vulnerability remediation priorities of the military Cyber Defence technicians in accordance with the NCISG Vulnerability Management SOPs and CD engineer directions.

6. Provides Level 2 Cyber Defense support to Deployed CIS.

7. Supporting Defensive Cyberspace Operations (DCO) during operations and exercises, while working at the DCIS Support Group (DSG) and in coordination with the NCISG HQ Cyber Defence engineers.

8. Supporting and guiding the incident response actions of the military Cyber Defence technicians deployed forward in support of operations and exercises in accordance with the NCISG Incident Response SOPs and CD engineer directions.

9. Investigating security incidents and, in coordination with the NSB HQ S-2/6 and NATO CIS Group HQ, supporting appropriate actions.

10. Developing, implementing and disseminating security awareness material and training for supported users in coordination with the NSB HQ S-2 and NATO CIS Group HQ.

11. Assisting the resolution of technically challenging problems with the cyber defence services installed in the deployable networks and systems.

12. Supporting Cyber Defense system installation, configuration and accreditation processes.

13. Participates in meetings, workgroups and projects with different NATO stakeholders as NSB Cyber Defence SME.

14. Supporting NSB Engineering Cell, NCISG J2/6 and NATO CyOC, within own AoR.

3. Special Requirements and Additional Duties

The incumbent 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. This a mandatory deployment post. The incumbent may be required to undertake deployments in support of military operations and exercises, and/or TDY assignments, both within and outside NATO's 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.

Mandatory Deployment Post. 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.

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 / risk might increase when deployed.

4. Essential Qualifications

a. Professional/Experience

1. Two years of demonstrable experience in the administration of Microsoft Workstation and Server systems, including
the management of Active Directory Domains, Group Policy objects and use of the PowerShell

console.
2. One year of demonstrable experience in UNIX/LINUX environments.
3. At least 2 years of experience supporting the security of Computer Systems and networks, either as a securityfocused
administrator or as a member of a Security Operations Center (SOC).
4. Deep knowledge and understanding of TCP/IP stacks, protocols, and ports.
5. Work experience in the use of computer security tools and vulnerability assessment methodologies.
6. Comprehensive knowledge of the principles of computer and communications security, networking, and the
vulnerabilities of modern operating systems and applications.
7. General certification in Information Assurance or CIS security (Security+, CCNA Security, GSEC, CEH, CISSP or equivalent).

b. Education/Training
Higher Secondary education and intermediate vocational training in computer science, engineering disciplines,
statistics or similar numerate discipline, operations research. or related discipline which might lead to a formal
qualification with 2 years experience, or Secondary education and completed advanced vocational training in that
discipline leading to a professional qualification or professional accreditation with 4 years post related experience.

c. Language

English - SLP 2222 - (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

1. Two years of work experience auditing computer systems, network infrastructure, web applications and applications.

2. Work experience in managing and configuring network equipment, firewalls, Intrusion Detection Systems and proxy servers.

3. Work experience with endpoint security and anti-malware management solutions (preferably the Trellix ePO management suite).

4. Work experience with SIEM applications (preferably Splunk).

5. Experience providing support and training to junior technical staff.

6. Experience in Vulnerability Assessment solutions and tools (Tenable.sc, Nessus, or equivalent).

b. Education/Training

1. Professional certification in the administration of Microsoft Windows or Linux operating systems (MCSA, RHCSA, Server+ or equivalent)

2. Professional certification in networking (CCNA, CCNP or equivalent)

• NATO C4ISR Orientation for Officers (CCC-SM-22206) provided by NATO Communications and Information Academy (NCI Academy)

• NATO Orientation Course (ETE-MW-3834) provided by NATO - School Oberammergau (NSO)

c. Language

None specified

6. Attributes/Competencies

• Personal Attributes: Since he works in Maintenance and Support Company and due to the fact he has to interact with the Battalion HQ and with the DCMs, a good leadership and a cooperative approach is required. Must be self reliant in resolving all technical matters regarding work. Able to think clearly and calmly under pressure. Ability and experience to provide on the job training. Ability to assess technical situations and take appropriate action or recommend solutions.

• Professional Contacts: The incumbent will have contact within NSB, and DCMs IS specialists.

• Contribution To Objectives: The position directly involves the Cyber Defence related operations and maintenance which affects the NSB's mission accomplishment both in a static peace headquarters and a deployed capacity.

There are no reporting responsibilities. This post reports to: Section Head (Mob CIS and Cyber Defence) - OR-8. This post does not deputises anybody. This post is not deputised by anybody.

7. Remarks

During crisis of MLE the incumbent is reassigned to the Crisis Establishment, where will carry out functions within the DCIS Support Group.

8. 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 **Grazzanise, Italy.** Note that once you created your profile, you will be able to use it to apply for other vacancies within NATO.

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 Adviser 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.