Duty Location **Mons, BEL**

:

JOB DESCRIPTION

Cell Head (Crypto Capability Validation)

NATO Cyber Security Centre

Grade: **G-17**

This is a position within the NATO Communications and Information NCIA, an organization of the North Atlantic Treaty Organization (NATO).

The NCIA has been established with a view to meeting to the best advantage the collective requirements of some or all NATO nations in the fields of capability delivery and service provision related to Consultation, Command & Control as well as Communications, Information and Cyber Defence functions, thereby also facilitating the integration of Intelligence, Surveillance, Reconnaissance, Target Acquisition functions and their associated information exchange.

The NATO Cyber Security Centre (NCSC) is responsible for planning and executing all lifecycle management activities for cyber security. In executing this responsibility, NCSC provides specialist cyber security-related services covering the spectrum of scientific, technical, acquisition, operations, maintenance, and sustainment support, throughout the lifecycle of NATO Information Communications and Technology (ICT). The NCSC enables secure conduct of the Alliance's operations and business in the context of NATO's C4ISR. The NCSC provides cyber security services to NCIA customers and users, as well as to all other elements of the Agency; this includes all Service Lines, Programme Offices, CIS Support Units/Elements, and the Agency Ops Centre.

The Infrastructure Branch delivers a suite of enabling services in the specific areas of Cryptography, Identity Management, Technical Services (supporting CS Operations) and CIS Protection. These services include capability and validation of NATOs crypto solutions, lifecycle management of cryptographic equipment and keys, operation and logistic support for NATO-wide online and offline cryptographic equipment, identity management services, gateway services, specialized enterprise-wide CS infrastructure (including NCIRC elements), application, configuration and management of NATO Enterprise-wide endpoint security software.

The Crypto Services Section ensures lifecycle management of cryptographic equipment, keys provision for high grade Crypto, operation and logistic support for NATO-wide online and offline cryptographic equipment, Cryptographic implementation and site surveys. The section is also responsible for Crypto Compliance includes Crypto Facility/Maintenance Inspections and Crypto installations validation. The Identity Management/PKI Services Section provides Certificate Authority, Revocation and Lifecycle Management of digital certificates/entities and the appropriate training of registration authority personnel.

The Crypto Capability Validation Cell as the NATO Cryptographic Installation Authority, is responsible for advising, certifying, and implementing end to end new secure system installations and cryptographic facilities, including site surveys in support of project.

Duties:

Under the direction of Crypto Services Section Head, the incumbent will perform duties such as the following:

- Provides the following:
    - project planning, coordination, testing and resource management;
    - the lead on site surveys, integrations/installations and inspections of cryptographic systems for secure end to end services;
    - focal point for subject matter expertise, and helpdesk in support of cryptographic issues;
    - build and test prototype IA designs to support new/modified requirements such as deployable and static secure CIS;
    - Advice and guidance to NCIA Project and System Managers during the whole life cycle of NATO CIS as well as providing subject matter related briefings and presentations.

- Responsible for the day to day management of the implementation team responsible for the installation and commissioning of all crypto equipment in NATO, in support of NATO HQ, Bi-SCs, NATO Nations, and NATO Operations and Exercises.
- Conduct the review of and input to capability packages as well as TBCEs and other estimation of efforts regarding NATO CIS projects;
- Development, production and maintenance of User Operator Guides and User Maintenance for NATO cryptographic systems;
- Development and production of semi-formal training package during initial installation of NATO cryptographic equipment and systems;
- Produce and provide reports and documentations for the relevant Security Accreditation Authorities as part of the security accreditation process;
- Deputize for higher grade staff as required;
- Perform any other duties as may be required.

Essential Experience and Education:

- A minimum requirement of a Bachelor's degree at a nationally recognised/certified University in a related discipline and 3 years post-related experience. Or exceptionally, the lack of a university degree may be compensated by the demonstration of a candidate's particular abilities or experience that is/are of interest to NCIA, that is, at least 10 years extensive and progressive expertise in duties related to the function of the post.
- Good knowledge and experience (at least 3 years) in the following areas:
    - Planning, design and implementation of security components of major CIS.
    - COMSEC/INFOSEC engineering of information or communication systems, including fully up-to-date technical knowledge related to future developments in the field of COMSEC equipment and systems, as well as INFOSEC practices and familiarity with related international, commercial and industrial standards;
    - Working experience in the Security Accreditation domain and change management related to acquisition and/or development projects for a large organization;
    - Very good knowledge of modern communication and Internet Protocol (IP) based networking technologies and systems including security aspects;
    - Extensive experience in the analysis of risks and the implementation and integration of INFOSEC protective measures;
    - Working knowledge of the operation of communications systems and troubleshooting techniques, Crypto accounting and distribution systems.

Desirable Experience and Education:

- Knowledge of NATO Security Policy and supporting directives;
- Prior experience of working in an international environment comprising both military and civilian elements;
- Graduate diploma in an INFOSEC related discipline;

- Background in cryptographic network management and electronic key management;
- Experience in development and implementation of computer security policies;

- Knowledge of NATO responsibilities and organization, including Allied Command Operations (ACO) and Allied Command Transformation (ACT);
- Experience in evaluation, audits, and accreditation of telecommunications and information systems;
- Practical experience leading installation teams on large project;
- Knowledge in emerging and disruptive technologies, especially IPv6, quantum resiliency, next generation networks;
- ITIL V3/V4 Certification;
- Prince2 Certification.

Language Proficiency:

- A thorough knowledge of English, both written and spoken, is essential and some knowledge of the other is desirable.
- **NOTE:** Most of the work of the NCIA is conducted in the English language.

Competencies or Personal Attributes:

- Planning and Organising - Sets clearly defined objectives for team members; plans activities and projects well in advance and takes account of possible changing circumstances; identifies and organises resources needed to accomplish tasks; manages time effectively; monitors performance against deadlines and milestones, manages service delivery risks and risks mitigations.
- Delivering Results and Meeting Customer Expectations - Focuses on customer needs and satisfaction; sets high standards for quality and quantity; monitors and maintains KPIs, service quality and productivity; works in a systematic, methodical and orderly way; consistently achieves project goals.