Duty Location: **Brunssum, NLD**

JOB DESCRIPTION
Section Head (Security)

Chief Service Operations - CIS Sustainment Support Centre

Grade: **G15**

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

To strengthen the Alliance through connecting its forces, the NCIA delivers secure, coherent, cost effective and interoperable communications and information systems in support of consultation, command & control and enabling intelligence, surveillance and reconnaissance capabilities, for NATO, where and when required. It includes IT support to the Alliances' business processes (to include provision of IT shared services) to the NATO HQ, the Command Structure and NATO Agencies.

The Chief Service Operations (CSO) is accountable to plan, operate and maintain Communication Information Systems (CIS) services throughout the allocated Area of Responsibility (AOR). CSO is to foster and sustain the highest levels of customer relationship with the operational user community. Additionally CSO is to exercise best business operations between the operational user-facing CIS support units to under-pin infrastructure services delivered by the NCI Agency Service Owners (SOs). CSO is responsible for all Asset Management (AM), the logistical support for all NATO owned CIS equipment, the Enterprise Service Operations Centre (ESOC) as well as the CIS Sustainment Support Centre (CSSC).

The CSSC is accountable to provide 3rd level maintenance capabilities for designated NATO CIS equipment, systems and associated non-CIS. In addition, it provides technical assessment capabilities limited engineering design and project management services. CSSC is also the Central CIS Hardware AM & supply hub within the NCI Agency.

The CSSC Management & Support Branch (CMSB) enables the Commander CSSC to direct, command, and coordinate all sustainment support actions to ensure efficient operations and business continuity as well as managing internal resources and equipment in accordance with NATO ICT policies, Integrated Logistic Support Plans (ILSPs), and NCI Agency tasking and directives. CMSB supports CSSC on all Security aspects, including Crypto maintenance and Crypto supply functions, as well as Health & Safety and Risk Management.

The Office of Security (OoS) is responsible for the facilitation and provision of the full-spectrum of CSSC Security services to CSSC in all locations in order to protect and defend NCIA personnel, facilities, resources and information from threats posed by terrorism, espionage, sabotage, subversion and any catastrophic incident/disaster. This includes management and execution of Physical Security, Personnel Security, Industrial Security, Security of Information, CIS Security, Counter Intelligence and Supply Chain Security. OoS manages all aspects of Cryptographic related equipment stemming from repair and maintenance to Depot-level support for the accounting, movement control and supervision. In terms of Cryptographic equipment volumes, management activities and storage - OoS is recognized as the 2nd largest NATO CCI account and largest Crypto Forward Support Point (CFSP).

The Head OoS is responsible for the day-to-day administration and efficient operation of the CSSC Security Section, with particular emphasis on physical security, security of information, access control, personnel security, and emergency planning within CSSC Brunssum. The incumbent is responsible for the leadership and management of personnel dealing with a wide range support tasks that are essential for the smooth and uninterrupted CSSC Service Delivery. Head OoS is also responsible for the coordination and oversight of Health & Safety and Risk Management activities and facilitates the provision and maintenance of safe working environment(s) for the whole CSSC workforce.

Duties:

Under the direction of the Branch Head CMSB the incumbent will perform duties as the follows:

- Responsible to the Branch Head CMSB for providing timely subject matter expert advice and support to senior management and staff based in CSSC on all protective security, personnel security, security of information, CIS Security issues, project and industrial security matters as they affect CSSC personnel and facilities;
- Responsible for the day-to-day administration, supervision and efficient operation of the CSSC OoS (Office of Security), with particular emphasis on Physical, Personnel, Industrial and overall Business security, as well as security of information, access control, visitor(s) management, CIS security, emergency planning and response to incidents and CRYPTO management;
- Responsible for managing and executing the Security Awareness programme for all CSSC personnel;
- Provide technical support in relation to CSSC security and Information Assurance (IA) related projects. This includes but is not limited to writing and reviewing IA requirements and specifications, contributing to technical documentation and evaluating and review of the accreditation process and needs;
- Create, develop and maintain local CSSC procedures in order to comply with NCI Agency and NATO CIS Security and IA Policies;
- Investigate and Manage all CSSC Security and IA incident investigations, providing reports and recommendations through the Head CMSB to the CSSC Commander and where necessary Agency Security Management Officer;
- Develop Physical and Electronic Security procedures for CSSC in line with NATO and NCI Agency Policies;
- Perform Annual Security Risk Assessments of the CSSC Estate;
- Conduct and support security inspections/audits;
- Oversight as COMSEC Officer planning and management of COMSEC activities within the CSSC;
- Performs pre-inspection of Crypto Facility;
- Ensures that all personnel requiring Crypto access receive proper briefing and training at the commencement of their duties and at the intervals required by the applicable Security Directives.
- Ensures that documentation of the Crypto access briefing and training is maintained in a permanent part of the crypto facility files;
- Monitors the security clearance status of personnel granted crypto access and suspends or revokes access upon demonstrated adverse behaviour;
- Contribute and support unit electronic emanations (TEMPEST) program establishment, implementation and compliance in accordance with NCIA COMSEC TEMPEST Technical and Implementation Directives.
- Support the development and management of the CSSC Business Continuity and Disaster Recovery and Emergency Evacuation and Destruction Plans;
- Provide support and SME expertise in the delivery of Internal IT Support to the CSSC personnel;
- Provides input for budget management of all security related equipment, Fire Safety equipment, mandatory internal and external security and safety training, physical security equipment, individual and professional development training;
- Attend and contribute to Internal NCIA and External Customer meetings as directed by Commander CSSC;
- Participate in the recruitment and selection of security staff including chairing, where appropriate, interview boards;
- Deputize for higher grade staff, if required;
- Performs other duties as required.
- The incumbent will undertake and perform Health and Safety Coordinator and Risk Management functions for CSSC and the Forward Support Points (FSPs).

Experience and Education:

- A Bachelor's degree at a nationally recognised/certified University in a relevant discipline such as IT Security, Facility Security, Industrial Security, or Communications Security and 2 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 NCI Agency, that is, at least 6 years extensive and progressive expertise in duties related to the function of the post;
- A minimum of 2 years working in and managing protective security, counter intelligence, physical protective security, Security of Information, CIS security, Personnel Security, IA, Security Education, BCP and Force Protection.
- Experience in applying and maintaining specific security controls as required by organizational policy and local risk assessments to maintain confidentiality, integrity and availability of business information systems.
- Experience in a field of Business security, COMSEC/INFOSEC CRYPTO and Security of Information.
- Knowledge of computer security and application of information access restrictions according to "need to know" principles.
- INFOSEC/COMPUSEC certification;

Desirable Experience and Education:

- Exceptionally, a combination of civilian/military qualifications and experience in all security fields.
- Formal qualification and certification in management, security, IA and Business Continuity management and planning;
- Trained and experienced in multi-national working groups, conferences and committees in a dynamic and changing environment;
- Prior experience of working in an international environment comprising both military and civilian elements;
- NATO CIS Security Officer Course;
- NATO Security Course;
- NATO Defence against Terrorism Course:
- Crypto Administration or COMSEC Engineering Course;
- ITIL knowledge and certification;
- Health & Safety Management certification
- A good working knowledge in development and implementation of CIS Security planning and evaluation and accreditation of telecommunications and information systems;
- Knowledge of NATO responsibilities and organization, including ACO and ACT.

Language Proficiency:

- A thorough knowledge of one of the two NATO languages, 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:

- Relating and Networking - Easily establishes good relationships with customers and staff; relates well to people at all levels; builds wide and effective networks of contacts; uses humour appropriately to bring warmth to relationships with others.
- Deciding and Initiating Action - Takes responsibility for actions, projects and people; takes initiative and works under own direction; initiates and generates activity and introduces changes into work processes; makes quick, clear decisions which may include tough choices or considered risks.

- Adhering to Principles and Values - Upholds ethics and values; demonstrates integrity; promotes and defends equal opportunities, builds diverse teams; encourages organisational and individual responsibility towards the community and the environment.
- Adapting and Responding to Change - Adapts to changing circumstances; tolerates ambiguity; accepts new ideas and change initiatives; adapts interpersonal style to suit different people or situations; shows an interest in new experiences.

Travel:

- Business travel to NATO and national (NATO and non-NATO) facilities as well as frequent travel between the NCIA offices;
- The employee 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.