



Duty Location: Brussels, Belgium

JOB DESCRIPTION

Principal Assistant (CIS Security)

Directorate of CIS Support Units – CSU Brussels

Grade: **G12**

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

To strengthen the Alliance through connecting its forces, the NCI Agency 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 Directorate of CIS Support Units (DCSU) is responsible to manage, deliver and maintain assigned Communications and Information System (CIS) products and services for the Agency's customers including NATO Headquarters (NHQ), the NATO Command Structure (NCS), NATO Force Structure (NFS), Nations and internal Agency users. DCSU provides liaison, planning and coordinating functions for Alliance Missions, Operations and Exercises. Services are delivered in coordination with the Enterprise Service Operations Centre (ESOC) and Agency Service Lines/Service Centres under the Enterprise Service Delivery Model (ESDM).

NCI Agency CIS Support Unit (CSU) Brussels, located in Brussels (BEL) is the primary Information, Communications and Technology (ICT) service provider for 24/7 support to the Secretary General, the International Staff (IS), the International Military Staff (IMS) and other Customers in the NATO Headquarters in Brussels. CSU Brussels enables end-to-end CIS services as it installs, operates, maintains and supports the full range of CIS capabilities during peacetime, crisis and war throughout its allocated Area of Responsibility (AOR) and as otherwise directed.

The Service Management Branch (SMB) supports the Agency's Demand Management (DM), Operations Centre, and Service Lines, and is responsible for liaison with all NCI Agency customers in the CSU's AOR and supports the Head CSU in the role as NCI Agency representative and provides a single entry point for customers. SMB contributes and/or conducts monitoring and measurement of customer satisfaction. SMB supports the management of all agreements concerning Service Provision, Operations and Exercises within the CSU AOR. SMB supports Service Lines in the implementation and improvement of service management processes. This branch directs, co-ordinates and supervises all activities of CSU's assigned resources in support of Exercises, Operations, Plans, Requirements, Project and Service Management. SMB reports appropriate Key Performance Indicators to Service Lines on a regular basis. The SMB is the interface to NATO HQ Information and Communication Technologies Management (ICTM) for programs and projects management and specifically serves as the local governance authority ensuring that NATO HQ standards and procedures are applied. SMB is also locally responsible for the integration of new or changed systems into the local baseline in compliance with the CSU Brussels Change Management process and provides the Configuration Management service to NATO HQ. This section integrates of new or changed systems into the local baseline in compliance with the CSU Brussels Change Management process. It provides the Configuration Management, CIS Architecture and CIS INFOSEC services to NATO HQ on a routine basis to fulfil the Service Level Agreement (SLA) with NATO HQ.

NATO UNCLASSIFIED

Duties:

Under the direction of the Branch Head, the incumbent will perform duties such as the following:

- Applies NATO Policies and Guidelines for all aspects of Information Assurance and keeps knowledge thereof up-to-date;
- Develops, implements and executes Security Test and Verification Plan (STVP);
- Creates reports documenting the STVP execution for issuance to the CIS Security Accreditation Authority (SAA) and the CIS Operational Authority (OA);
- Supports the development, traceability and versioning of security related documentation (CSRS, SSRS, SISRS, SecOPs, SRA, etc.);
- Liaises with other parts of the Organisation for current situational awareness in the field of Information Assurance;
- Supports the monitoring of the correct implementation of security mechanisms within the (sub) organisation;
- Supports control and compliance initiatives (e.g. Vulnerability Assessment, self-assessment, third party reviews);
- Supports technical discussions related to work package development, reviews and assessments, including CIS security;
- Supports other parts of the CSU such as IT Service Continuity Management (ITSCM), Business Continuity and Disaster Recovery Plan(s), and Continual Service Improvement initiatives;
- Plans, manages, coordinates and conducts work to meet quality targets;
- Takes initiative to investigate, diagnose and resolve issues in a systematic approach;
- Maintains sound knowledge in the area of work;
- Assists his/her superiors and recommends solutions;
- Works on own initiative with limited supervision, and possibly leads others as required;
- Deputizes for higher grade staff, if required;
- Performs other duties as may be required.

Experience and Education:

- Higher vocational training in a relevant discipline with 3 years post-related experience, or a secondary educational qualification with 5 years post-related experience;
- Experience in monitoring the provision of CIS Security services on a variety of platforms including firewalls, servers, routers, hubs and workstations;
- Experience in coordinating complex discussion concerning IT requirement review for implementation;
- Experience with Security Test and Planning including execution and reporting;
- Knowledge of a broad range of CIS Security disciplines;
- Certified ITIL Foundation or higher.

Desirable Experience and Education:

- Experience working within classified network environments;
- Practical experience in identifying appropriate computer security tools usable in classified environments, and implementing them to support system operations;
- Expertise in operating an effective intrusion detection system;
- Experience using a formal project management approach (preference PRINCE2) with team members coming from a matrix management structure;
- Experience in managing business and IT requirement throughout life-cycle;
- Good knowledge of current Windows Server and Workstation OS and Router/Switch configuration (preference CISCO);
- Good knowledge of TCP/IP protocols;
- Knowledge of a NATO CIS Security Policy, Directive and Guidance or the readiness to acquire this as soon as practicable after appointment;
- Prior experience of working in an international environment comprising both military and civilian elements;
- Knowledge of NATO responsibilities and organization, including ACO and ACT.

Language Proficiency:

NATO UNCLASSIFIED

- 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 NCI Agency 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;
- **Delivering Results and Meeting Customer Expectations** -- Focuses on customer needs and satisfaction; sets high standards for quality and quantity; monitors and maintains quality and productivity; works in a systematic, methodical and orderly way; consistently achieves project goals;
- **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;
- **Achieving Personal Work Goals and Objectives** -- Accepts and tackles demanding goals with enthusiasm; works hard and puts in longer hours when it is necessary; seeks progression to roles of increased responsibility and influence; identifies own development needs and makes use of developmental or training opportunities.