



## JOB DESCRIPTION

### Post Details:

Post Title:	<b>Engineer (Crypto Validation)</b>	Organisational Element:	NCSC
		Job Family:	Cyber Security Engineering
Rank/Grade:	G15		
Military/Civilian:	Civilian	Location:	Mons, BE

### Organisation context:

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.

### Organisational Element Statement of Functions:

The NATO Cyber Security Centre (NCSC) delivers full lifecycle cyber services to enable the secure execution of NATO's consultation, operations, and missions and enhance the Alliance's collective cyber defence.

As its principal provider of cyber services, the NCSC makes NATO more resilient to cyber threats, protecting and defending Communications and Information Systems (CIS) through centralized and round-the-clock services. The NCSC also leads the implementation of new cyber capabilities within NATO and supports other Business Areas in the implementation and delivery of cybersecurity projects and services. In addition to delivering services and managing projects, the NCSC also provides the technical hands-on-keyboard experts for the conduct of Defensive Cyber Operations (DCOs).

Core activities include, inter alia, technical design, guidelines development, accreditation support, cybersecurity capabilities management, vulnerability assessment and remediation support, operating the NATO Public Key Infrastructure, malicious activity detection, threat hunting, incident response, information sharing, TEMPEST zoning, management of cryptographic systems, penetration testing, purple and red teaming, and defensive cyber operations including maintaining a rapid reaction team. It also tracks research and pursues innovation in cyber.

The NCSC is the centre of technical expertise for cyber within the Alliance and leads information sharing and collaboration initiatives at the technical level within the Alliance and with external stakeholders.

The NCSC is part of the nucleus of the NATO Integrated Cyber Defence Centre (NICC).

**Job role description:**

A Cyber Security Infrastructure Specialist is responsible for designing, implementing, and maintaining an organization's security infrastructure. They identify potential security vulnerabilities and develop strategies to mitigate them. They also monitor and analyze security systems to detect and respond to security incidents. This role requires expertise in network security, firewalls, intrusion detection and prevention systems, and other security technologies.

**Duties and Responsibilities:**

**Information security:**

- Applies and maintains specific security controls as required by organisational policy and local risk assessments.
- Communicates security risks and issues to business managers and others.
- Performs basic risk assessments for small information systems.
- Contributes to the identification of risks that arise from potential technical solution architectures.
- Suggests alternate solutions or countermeasures to mitigate risks.
- Defines secure systems configurations in compliance with intended architectures.

**Information assurance:**

- Follows standard approaches for the technical assessment of information systems against information assurance policies and business objectives.
- Makes routine accreditation decisions.
- Recognises decisions that are beyond their scope and responsibility level and escalates according.
- Reviews and performs risk assessments and risk treatment plans.
- Identifies typical risk indicators and explains prevention measures.
- Maintains integrity of records to support and justify decisions.

**Risk management:**

- Undertakes basic risk management activities.

**Technology service management:**

- Takes responsibility for managing the design, procurement, installation, upgrading, operation, control, maintenance and effective use of specific technology services.
- Ensures adherence to relevant policies and procedures.
- Ensures that processes and practices are aligned across teams and providers to operate effectively and efficiently.
- Provides appropriate status and other reports to managers and senior users.

**Incident management:**

- Provides first line investigation and gathers information to enable incident resolution and allocate incidents.
- Advises relevant persons of actions taken.

**Additional duties for this post:**

- Secure Infrastructure Management
- Network Support (NTAS)

- Infrastructure Operations (ITOP)

### **Education, Experience and Training (essential):**

#### **Education:**

A minimum requirement of a Bachelor's degree at a nationally recognised/certified University in a related discipline 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 NCIA, that is, at least 6 years extensive and progressive expertise in duties related to the function of the post.

#### **Experience:**

- At least 2 years practical experience of designing, implementing, and maintaining security infrastructure.
- Practical experience identifying and mitigating security vulnerabilities.
- Extensive knowledge in network security hardware - firewalls, intrusion detection and prevention systems.
- Extensive knowledge of network protocols, encryption technologies, and specific experience with cryptographic equipment.
- Ability and desire to stay up to date with the latest security technologies and trends.
- Strong communication and analytical skills.
- Security Accreditation of major CIS acquisition and/or development projects for a large organization.
- Security risk assessment methodologies and tools.
- 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/industrial standards.
- Working experience in the Security Accreditation domain and change management related to the implementation of major CIS acquisition and/or development projects for a large organization.

### **Education, Experience and Training (desirable):**

#### **Experience:**

- Knowledge of NATO Security Policy and supporting directives.
- Prior experience of working in an international environment comprising both military and civilian elements.
- Technical background in the Information Systems Security and Cryptographic systems.
- Knowledge of NATO responsibilities and organization, including Allied Command Operations (ACO) and Allied Command Transformation (ACT).
- Practical experience leading installation teams on large projects.

#### **Training/Certifications:**

- CompTIA Security+

- CISCO Certified Network Associate (CCNA)
- NATO CIS Security Officer (NCI Academy – 0280)
- NATO COMSEC System Engineering (NCI Academy – 0067)

**Behavioural competencies:**

- *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.
- *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.
- *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.

**Language:**

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.

**Travel:**

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

May be required to undertake duty travel to operational theatres inside and outside NATO boundaries

**Work Environment:**

The work is normally performed in a typical Secure Facility environment. Slightly Undesirable Conditions apply. The risk of injury is categorised as Light Risk of Injury. Occasionally military exercise or operations environment.