JOB DESCRIPTION

Post Details:			
Post Title:	**Senior CIS Security Officer**	Organisational Element:	NCSC
		Job Family:	Information Security Management
Rank/Grade:	G17		
Military/Civilian:	CIV	Location:	Mons/BEL

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:

Keeps tracks of CIS threats and updates other members of the team accordingly. Evaluates application configurations and advises on security Issues. Participates in investigations that require electronic information. Develops and implements Data Loss protection procedures and practices. Monitors security systems, investigates incidents, and enforces policies to protect information and assets from cyber threats.

Duties and Responsibilities:

Information security:

- Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards.
- Contributes to development of information security policy, standards and guidelines.
- Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems.
- Investigates major breaches of security, and recommends appropriate control improvements.
- Develops new architectures that mitigate the risks posed by new technologies and business practices.

Information assurance:

- Interprets information assurance and security policies and applies these to manage risks.
- Provides advice and guidance to ensure adoption of and adherence to information assurance architectures, strategies, policies, standards and guidelines.
- Plans, organises and conducts information assurance and accreditation of complex domains areas, cross-functional areas, and across the supply chain.
- Contributes to the development of policies, standards and guidelines.

Threat intelligence:

- Performs routine threat intelligence gathering tasks.
- Transforms collected information into a data format that can be used for operational security activities.
- Cleans and converts quantitative information into consistent formats.

Governance:

- Implements the governance framework to enable governance activity to be conducted.
- Within a defined area of accountability, determines the requirements for appropriate governance reflecting the organisation's values, ethics and wider governance frameworks.
- Communicates delegated authority, benefits, opportunities, costs, and risks.
- Leads reviews of governance practices with appropriate and sufficient independence from management activity.
- Acts as the organisation's contact for relevant regulatory authorities and ensures proper relationships between the organisation and external stakeholders.

Risk management:

- Plans and implements complex and substantial risk management activities within a specific function, technical area, project or programme.
- Implements consistent and reliable risk management processes and reporting to key stakeholders.
- Engages specialists and domain experts as necessary.
- Advises on the organisation's approach to risk management.

Consultancy:

- Takes responsibility for understanding client requirements, collecting data, delivering analysis and problem resolution.

- Identifies, evaluates and recommends options.
- Collaborates with, and facilitates stakeholder groups, as part of formal or informal consultancy agreements.
- Seeks to fully address client needs and implements solutions if required.
- Enhances the capabilities and effectiveness of clients, by ensuring that proposed solutions are fully understood and appropriately exploited.

Incident management:

- Ensures that incidents are handled according to agreed procedures.
- Prioritises and diagnoses incidents.
- Investigates causes of incidents and seeks resolution.
- Escalates unresolved incidents.
- Facilitates recovery, following resolution of incidents.
- Documents and closes resolved incidents.
- Contributes to testing and improving incident management procedures.

Security operations:

- Monitors the application and compliance of security operations procedures.
- Reviews actual or potential security breaches and vulnerabilities and ensures that they are promptly and thoroughly investigated.
- Recommends actions and appropriate control improvements.
- Ensures that security records are accurate and complete and that requests for support are dealt with according to agreed procedures.
- Contributes to the creation and maintenance of policy, standards, procedures and documentation for security.

Vulnerability assessment:

- Plans and manages vulnerability assessment activities within the organisation.
- Evaluates and selects, reviews vulnerability assessment tools and techniques.
- Provides expert advice and guidance to support the adoption of agreed approaches.
- Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems.

Additional duties for this post:

- Act as the NCSC CIS Security Officer.
- Develop and oversee security awareness and training programs to ensure that all employees are aware of their role in maintaining information security.
- Monitor and analyse security incidents and threats, and develop and implement incident response plans in collaboration with Incident Management Team.
- Develop and maintain relationships with key stakeholders, such as senior management, external auditors, and regulatory authorities.
- Assists in the development and maintenance of disaster recovery and business continuity plans.
- Manage and oversee third-party vendors and service providers to ensure that they meet security requirements.
- Conduct regular security audits and assessments to ensure that the NATO Cyber Security Centre is compliant with security standards.

- Responsible for coordinating with leadership during security incidents and participating in the response and recovery efforts.
- Liaison with government and non-government Computer Emergency Response Teams (CERTs) and other specialist organisations.
- Integrate into the Change Management Process to advice the Change Management Board on security risks during prescribed meetings (Distributed CAB, Technical Review Board, etc.).
- Participates in the Accreditation Process of NCSC networks and systems and provide security feedback to NATO Security Accreditation boards.
- Deputizing for higher grade staff, if required.
- Performing other duties as may be required.

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 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.

Experience:

- Comprehensive knowledge of the principles of computers and communication security, networking, and the vulnerabilities of modern operating systems and applications.
- Experience with implementation and integration of CIS Security protective measures in enterprise environments.
- Experience in governance, risk, and compliance (GRC).
- Leading security audits, risk assessments, and regulatory reporting.
- Developing and maintaining security frameworks (ISO 27001, NIST, CIS).
- Enforcing organization-wide policies and defining security awareness programs.
- Cross-functional collaboration with other Business areas and Functional areas of the organisation.
- Liaison between technical and business teams.
- Overseeing and support testing, disaster recovery and business continuity capabilities.
- Responding to and knowledge of security investigation and initial response capabilities.

Education, Experience and Training (desirable):

Experience:

- Knowledge of cryptographic and emission security concepts\ knowledge of NATO security policy.
- Prior experience of working in an international environment comprising both military and civilian elements.
- Knowledge of NATO responsibilities and organization, including its strategic commands (i.e., ACO and ACT).

Training/Certifications:

- Certifications such as CISSP, CISA, or CRISC are considered an asset for this role.
- NATO CIS Security Officer training.

Behavioural competencies:

- *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.
- *Formulating Strategies and Concepts* - Works strategically to realise organisational goals; sets and develops strategies; identifies, develops positive and compelling visions of the organisation's future potential; takes account of a wide range of issues across, and related to, the organisation.
- *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.

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 frequent travel between the NCIA offices; – May be required to undertake duty travel to operational theatres inside and outside NATO boundaries.
Work Environment:	– Normal office environment. Normal working hours 0830-1730. On-call duties after working hours, on weekends or holidays are required. – Occasionally military exercise or operations environment. – The incumbent may be required to perform duties elsewhere within the organization as directed.