JOB DESCRIPTION

Post Details:			
Post Title:	**Principal Cyber Security Engineer**	Organisational Element:	NCSC
		Job Family:	Cyber Security Engineering
Rank/Grade:	G20		
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:

As a Principal Cybersecurity Engineer, your primary responsibilities will include designing and implementing agile, resilient cybersecurity solutions aligned with operational and business requirements. You will collaborate with stakeholders to translate functional needs into effective technical security solutions and oversee the design, integration, testing, operation, and maintenance of information system security throughout the systems development life cycle (SDLC).

In addition, you will coordinate with Heads of Branches and Sections to support strategic initiatives, projects, and business objectives, ensuring alignment with the Agency's overall strategic plan.

Duties and Responsibilities:

Solution architecture:

- Leads the development of solution architectures in specific business, infrastructure or functional areas.
- Leads the preparation of technical plans and ensures that appropriate technical resources are made available.
- Ensures that appropriate tools and methods are available, understood and employed in architecture development.
- Provides technical guidance and governance on solution development and integration.
- Evaluates requests for changes and deviations from specifications and recommends actions.
- Ensures that relevant technical strategies, policies, standards and practices (including security) are applied correctly.

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.

Requirements definition and management:

- Plans and drives scoping, requirements definition and prioritisation activities for large, complex initiatives.
- Selects, adopts and adapts appropriate requirements definition and management methods, tools and techniques.
- Contributes to the development of organisational methods and standards for requirements management.
- Obtains input from, and agreement to requirements from a diverse range of stakeholders.
- Negotiates with stakeholders to manage competing priorities and conflicts.

- Establishes requirements baselines.
- Ensures changes to requirements are investigated and managed.

User experience analysis:

- Determines the approaches to be used for user experience analysis.
- Plans and manages user experience and accessibility analysis activities.
- Provides expert advice and guidance to support the adoption and adaptation of agreed approaches.
- Develops user experience tools, techniques and standards as part of the organisation's framework for user-centred design.

Additional duties for this post:

- Overseeing the day-to-day operations, including delegating tasks and ensuring that all work is completed on time and to a high standard.
- Developing and implementing strategies to achieve goals and objectives, in line with the organisation's overall mission and vision.
- Perform other duties as may be required.
- Deputise for higher grade staff, if required.

Education, Experience and Training (essential):

Education:

A Master's degree at a nationally recognised/certified University in a related discipline and 5 years post-related experience. Or a Bachelor's degree with 8 years post related experience.

Experience:

- Remarkable l IT experience, including at least 5+ years in a senior leadership or deputy role managing multi-disciplinary engineering teams.
- Proven track record overseeing large-scale IaaS, PaaS, and NaaS environments (e.g., AWS, Azure, or private enterprise clouds).
- Experience managing Public Key Infrastructure (PKI), hardware security modules (HSMs), cryptographic key lifecycles, and data-at-rest/in-transit encryption standards.
- Experience managing extensive financial resources, and strictly enforcing vendor Service Level Agreements (SLAs).
- Proven experience managing teams, resources, projects and service delivery.
- Demonstrable knowledge in the development and use of Cyber Security Architectures, Technologies and Tools in securing Enterprise Level CIS environments.
- Experience of high-assurance cryptographic equipment, COMSEC (Communications Security) account management, and Key Management Infrastructure (KMI).

Training/Certifications:

- Holds, or have held, a nationally recognised qualification in Service Management, preferably ITIL V3, V4, V5 at Practitioner/Intermediate/Manager/Professional/Leader level.
- Holds, or have recently held, a nationally recognised qualification in CIS Leadership/Management.

Education, Experience and Training (desirable):

Education:

- A Master's degree in Computer Science, Information Technology, Enterprise Systems Engineering, Cyber Security or related subject.

Experience:

- Knowledge of Cryptographic mechanisms, and the foundational understanding of installing, operating and managing cryptographic products in an Enterprise environment.
- Knowledge of PKI mechanisms, and the foundational understanding of installing, operating and managing PKI products in an Enterprise environment.
- Knowledge of classified asset management, configuration management, and secure supply chain risk management (SCRM).

Training/Certifications:

- AWS certified solutions Architect (Professional) or Microsoft Certified Azure solutions Architect (Expert).
- CCNP/CCIE Enterprise
- TOGAF Enterprise Architecture
- GIAC Security Leadership
- PRINCE2/PMP

Behavioural competencies:

- *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.
- *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.
- *Leading and Managing* - Provides others with a clear direction ; motivates and empowers others; attracts and develops staff of a high calibre; provides staff with development opportunities and coaching; sets appropriate standards of behaviour.

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 may be required. In case of an enterprise-level Cyber Incident, the incumbent may be required to work extended hours.