26748 - Senior Cyber Security Engineer

Location: Mons, Belgium.

Period: 166 (start on 16 Dec. 2026)

Deadline: 10 Nov. 2026

Duties/Roles:

Solution architecture:

- Contributes to the development of solution architectures in specific business, infrastructure or functional areas.

- Identifies and evaluates alternative architectures and the trade-offs in cost, performance and scalability.

- Determines and documents architecturally significant decisions.

- Produces specifications of cloud-based or on-premises components, tiers and interfaces, for translation into detailed designs using selected services and products.

- Supports projects or change initiatives through the preparation of technical plans and application of design principles.

- Aligns solutions with enterprise and solution architecture standards (including security).

Cybersecurity:

- Provides guidance on the application and operation of elementary physical, procedural and technical security controls.

- Explains the purpose of security controls and performs security risk and business impact analysis for medium complexity information systems.

- Identifies risks that arise from potential technical solution architectures.

- Designs alternate solutions or countermeasures and ensures they mitigate identified risks.

- Investigates suspected attacks and supports security incident management.

Requirements definition and management:

- Defines and manages scoping, requirements definition and prioritisation activities for initiatives of medium size and complexity.

- Contributes to selecting the requirements approach.

- Facilitates input from stakeholders, provides constructive challenge and enables effective prioritisation of requirements Establishes requirements baselines, obtains formal agreement to requirements, and ensures traceability to source.

User experience analysis:

- Selects appropriate techniques and tools to develop user stories and elicit user experience requirements in complex situations.

- Identifies and describes the design goals for systems, products, services and devices.

- Identifies the roles of affected stakeholder groups.

- Resolves potential conflicts between differing user requirements.

- Specifies measurable criteria for the required usability and accessibility of systems, products, services and devices.

Project implementation responsibilities:

- Provides cyber security technical and professional input and technical leadership to engineering projects. These contributions will include, but are not limited to, statement of work preparation, execution planning, cyber items procurement, cyber security delivery effort coordination between assigned hands-on engineers within NCIA and NCSC by following multi-layer change management framework, problems identification and resolution, internal and external to NCSC quality control management, contribution to internal written and not written knowledge management, results' documentation (system post-implementation specifications, instructions, updates to cyber security services documentation), handover to NCSC cyber security services for operations and operations and maintenance costs calculations;

- Provides technical input and support to acquisition projects including, but not limited to, writing and reviewing / coordinating cyber security requirements (statement of work, system design specification, high and low level design blueprints, bill of material), supporting procurement process (providing answers to raised questions); evaluating bids;

General responsibilities

- Develops and presents cyber security scientific, engineering, technical, and marketing information suitable for official meetings.

- Represents the NCIA/ NCSC in working groups and forums.

- Executes tasks assigned by Branch, NCSC Service Delivery Managers and Resource manager.

Skills, Knowledge, Experience Required:

Mandatory:

- The candidate must have a currently active NATO SECRET security clearance;

- 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 those in this Statement of Work;

- At least 3 years practical experience developing or delivering services in Cybersecurity;

- Extensive practical experience identifying vulnerabilities and potential security threats;

- Development of technical requirements, system diagrams and other engineering products to aid Cybersecurity acquisition and procurement;

- Proven ability to deliver cyber security capabilities for industry, government, or military;

- Up to date knowledge and experience in design and implementation of cyber security capabilities and supporting infrastructure elements in an operational environment;

- Up to date knowledge and experience in cryptographic technologies including key management;

- Up to date knowledge and experience in identity and access management;

- Up to date knowledge and experience in risk management;

- Knowledge of network monitoring and detection technologies;

- Knowledge of the design of cyber security capabilities on cloud infrastructure;

- Ability to apply architecture methodologies to express complex, systems of systems in architectural terms and models of varying detail;

- Recognised track record in dealing with stakeholders, understanding their needs, problems, and requests and proposing constructive ways ahead;

- Proactive attitude in seeking and maintaining trust from stakeholders;

- Proven ability to communicate effectively orally and in writing with good briefing skills;

- Experience leading small teams;

- Very good communication and analytical skills;

- Language proficiency in English: meet or exceed the NATO STANAG 6001 Level 3 "Professional Proficiency";

- Proficient at using the ArchiMate modelling language;

- Relevant certifications in cyber security, such as Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP) or GIAC Security.

Desirable:

- Experience in working for or supporting a military or governmental organization.

Required Level of Security Clearance:

NATO SECRET.