

26598 - Senior Cyber Security Specialist

Location: Mons, Belgium.

Period: 395 (start on 30 Oct. 2026)

Deadline: 24 Sep. 2026

Duties/Roles:

- Install, configure and maintain the day-to-day NATO wide PKI systems and components;
 - Install, configure and maintain NATO PKI (NPKI) virtualized infrastructure;
 - Install, configure and maintain NPKI networking components;
 - Install, configure and maintain NPKI hardware infrastructure;
 - Install, configure and maintain NPKI LDAP directory service and support HTTP service;
 - Responsible for Enterprise Mobile Mobility configuration, integration, maintenance;
 - Responsible for LDAP directory service configuration and maintenance;
 - Responsible for Online Certificate Status Protocol (OCSP) and Time Stamp management;
 - Responsible for Database maintenance, dedicated for NPKI;
 - Responsible for Card Management System deployment, integration and day-to-day management;
 - Responsible for Hardware Security Module (HSM) firmware upgrade and management;
 - Responsible for the creation of PKI related guidance;
 - Certificate Authority Log analysis, (Troubleshoot the system ALARM/ERRORS and monitor user activity);
- Support Smart Card enrolment and certificate creation process;
- Maintain the day-to-day operations /management /backup/restore of the PKI systems;
 - Provide technical support and assistance to ITM Operating Authorities and NPKI-Mitigation project team;
 - Provide 2nd and 3rd level technical support of CIS services to the NPKI customers;
 - Designing of new PKI components;

- Responsible for the creation and maintenance of Standard Operating Procedures within the NPKI as part of modifications or additions to current capabilities;
- Documenting of all new PKI services;
- Installation and maintenance of NPKI components;
- Be flexible to work outside normal office hours in response to crises, operational requirements;
- Investigation of network faults, security incidents and performance issues, including the development and implementation of proposed improvements;
- Support to the integration of cyber security tools into existing and future NATO CIS environments;
- Conducting testing, validation and acceptance activities for deployed cyber security capabilities;
- Support to the development of technical documentation, including installation guides, configuration baselines, test plans, test reports, standard operating procedures and security hardening guides;
- Provision of technical advice and recommendations on cyber security architecture, tool configuration, system integration and operational improvements;
- Coordination with project managers, system engineers, network engineers, security architects and operational stakeholders to ensure successful delivery of cyber security capabilities;
- Ensuring that implemented solutions comply with applicable NATO security policies, operational requirements and agreed technical standards;
- Support to handover to operations, including knowledge transfer, training support and preparation of operational documentation;
- Participation in technical meetings, reviews, workshops and coordination activities with NATO, national and industry stakeholders.

Skills, Knowledge, Experience Required:

- 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 5 years practical experience in cyber security or related field, such as developing and maintaining cyber security solution architecture, developing or delivering capabilities and services in the area of Cyber security, or complex and demanding technical environments;
- Extensive knowledge of modern communication and Internet Protocol (IP) based networking technologies and systems including security aspects.
- Working knowledge of router and switches configuration.
- Practical experience in Windows Servers, RHEL and VMware system administration.
- Knowledge of the principles of computer and communications security, networking, and vulnerabilities of modern operating systems and applications.
- Experience with SQL database administration.
- Extensive experience in operating systems backup and restore.
- Practical experience in scripting (Python, PowerShell).
- Practical experience in automation (Ansible).
- Practical experience in SSL, TLS, and OpenSSL.
- Minimum 5 years of experience in the following areas:
- Installation, testing and integration of networks
- Network support, including experience with:
 - Network management software and tools to collect agreed performance statistics
 - Experience in carrying out agreed network maintenance tasks
 - Network migration projects
 - Identification and resolving network problems according to agreed procedures.
- Configuration, maintenance and repair of SAN, servers, tape libraries, VMware/ VSphere.
- Responsibility for installation projects, systems installation/decommissioning, monitoring the effectiveness of installations and developing and implementation of quality plans/method statements.
- System integration, defining the integration build, configuration of the hardware environment, producing integration test specifications, conducting tests, recording details of failures and carrying out fault diagnosis.
- Configuration management and applying tools, techniques and processes for administering configuration items.
- Experience with problem management, investigation of problems in systems and services and assistance with implementation of agreed solutions /preventative measures

- The contracted individual shall have recent and relevant experience with technologies and tools including Juniper, Palo Alto, RSA NetWitness.
- The individual shall also have experience in the design and configuration of IT infrastructure elements within projects, including routing, switching and virtualisation technologies such as VMware.
- The individual shall have a proven ability to deliver technologies, systems, solutions and capabilities for industry, government or military organisations, including deployment to operational military areas.
- Experience with implementation projects within NATO and/or national military organisations is desirable.
- The individual shall be capable of working independently and as part of a team to achieve agreed objectives, including the ability to monitor, coordinate and support industry teams. Excellent communication and technical writing skills in English are required.
- Very good communication and analytical skills.
- Language proficiency in English: meet or exceed the NATO STANAG 6001 Level 3 "Professional Proficiency".

Desirable:

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

Required Level of Security Clearance:

NATO SECRET.