26592 - Endpoint Security Assistant

Location: Mons, Belgium.

Period: 395 (start on 02 Nov. 2026)

Deadline: 21 Sep. 2026

Duties/Roles:

1. Software Lifecycle & Change Management Support

- Monitor vendor sites for software updates and tools;

- Download, package, and archive software releases (e.g., ZIP files);

- Prepare supporting documentation (product guides, release notes, change logs);

- Initiate and process internal Requests for Change (RFCs);

- Complete required internal approval documentation and compliance paperwork;

2. Shared Mailbox & Action Tracking

- Monitor and manage the team's group mailbox;

- Track pending requests and open items;

- Proactively follow up with engineers on unanswered emails and tickets;

- Send reminders and ensure no actions are missed;

- Maintain visibility of response status and closure.

3. Web Portal Content Management

- Maintain and update the team's web portal;

- Replace outdated versions of published materials;

- Ensure new releases are properly uploaded;

- Verify completeness of uploaded materials (e.g., release notes, change logs);

- Perform quality checks before publication.

4. Lab Environment Coordination

- Ensure lab environments are updated with latest approved software versions;

- Maintain correct configurations based on engineering guidance;

- Track version alignment between lab and production references.

5. Reporting & Post-Change Analysis

- Track implementation of configuration changes;

- Prepare follow-up reports (e.g., one week post-change);
- Analyze results using Excel (filtering, grouping, trend analysis);
- Summarize findings and present structured feedback to engineers;
- Highlight potential corrective actions.

6. Documentation & Process Governance

- Document internal procedures and workflows;
- Take meeting minutes and track action items;
- Maintain structured documentation repository;
- Ensure processes are consistently recorded and updated.

7. General Administrative & Operational Support

- Handle internal administrative requests (e.g., spreadsheets, reporting inputs);
- Support onboarding of newcomers;
- Coordinate visitor logistics (room bookings, paperwork, access coordination);
- Assist with operational organization tasks as required.

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 in an EDMS (Enterprise Document Management System);
- At least 3 years' experience with SharePoint content management;
- At least 3 years' experience with standard desktop tool like Office and Adobe Acrobat. Emphasis on Outlook use, calendar management, shared calendars and Outlook tasks;
- At least 1 years' experience with statistical analysis on Excel;
- Familiarity with NATO procedures and forms will be an asset;
- Familiarity with NATO structure will be an asset;

- Familiarity with cyber security concepts will be an asset;

- Familiarity with project management will be an asset;

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

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

- Strong organizational and follow-up skills;

- Self-motivated and "can do" attitude;

- Flexibility, tactfulness and dependability;

- Attention to detail and documentation accuracy;

- Ability to coordinate across technical and non-technical stakeholders;

- Proactive communication and task tracking;

- Very good communication and analytical skills;

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

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

- Relevant certifications in architecture and service delivery such as The Open Group Architecture Framework (TOGAF), ArchiMate modelling language, and ITIL.

Desirable:

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

Specific Working Conditions:

If working from a remote location, the contractor shall provide IT equipment for the processing of public and unclassified information in support of their duties, including the capability to participate in video meetings using Microsoft based collaboration tools.

The contractor may be permitted to perform work remotely, from a different NATO nation than the duty location, for up to a maximum of twenty percent (20%) of their total working time, subject to prior approval by their Resource Manager (to which they will be assigned upon contract start) and the section head. The contractor may work from their home in the duty location subject to the NCIA teleworking policy and in coordination with the section head.

.

Required Level of Security Clearance:

NATO SECRET.