Job Title: Ground Segment Cyber Security Engineer (2 posts)

Req ID **4323** - Posted **23/04/2018**

EUROPEAN SPACE AGENCY

Vacancy in the Directorate of Navigation.

ESA is an equal opportunity employer, committed to achieving diversity within the workforce and creating an inclusive working environment. Applications from women are encouraged.

Post
Ground Segment Cyber Security Engineer (2 posts)

This post is classified A2-A4 on the Coordinated Organisations' salary scale.

Location
ESTEC, Noordwijk, The Netherlands

Description

Ground Segment Cyber Security Engineer (2 posts) in the Galileo Ground Segment & Cyber Security Engineering Unit, Galileo Security Office, Navigation Security Office, Directorate of Navigation.

Duties
Reporting hierarchically to Head of Unit and functionally to Head of Galileo GS Procurement, the postholder performs these tasks:

- defining and implementing a cyber security management process (vulnerabilities identification, correction follow-up, mitigation) for Galileo Ground Segment (GS) infrastructure (GMS, GCS, GSF);
- providing cyber security expertise in terms of network security design for vulnerability short term and long-term mitigation via technology upgrades or proposing operational mitigation;
- managing cyber security vulnerabilities: proposing correction or mitigation, analysing criticality, performing associated risk scenario analysis;
- collecting and managing cyber vulnerabilities closure evidence for demonstration that vulnerabilities have been correctly mitigated for each version of the GS infrastructure;
- proposing tools for cyber vulnerabilities management;
- compiling and producing the monthly cyber status report for Galileo GS infrastructure and participating in the project Cyber Board to present the status;
- presenting cyber status and evidence to Galileo security accreditation authorities: Cyber Board, GSAP/SAB (Galileo Security Accreditation Panel / Security Accreditation Board);
- organising and following up security audits and penetration testing activities on GS infrastructure;
- assessing criticality of security audits and test findings;
- proposing plan for short/medium/long-term correction of critical findings;
- providing support for Galileo Security Monitoring (SECMON) design, development, AIV and accreditation follow-up activities, including interactions with relevant stakeholders (hosting entity, operations);
- supporting definition of security monitoring events collection strategy and correlation rules for control and mitigation of Galileo infrastructure vulnerabilities and risk scenario;
- participating in each GS delivery review and acceptance review assessing GS cyber status;
- participating as permanent member in the classified engineering boards and relevant CCBs;
- regular reporting to Head of Unit.

Technical competencies
Knowledge of large operations and associated software systems, preferably space-based
Experience in development and maintenance of ground infrastructure and/or software systems
Architecture of ground stations dedicated to space mission support
Galileo system and ground segment architecture
Cyber security (policy, detection, reaction, correction)
Security engineering, especially security monitoring
Network communications
Information technology security

Behavioural competencies
Communication
Planning & Organisation
Problem Solving
Teamwork

Education

Applicants should have a Master's or equivalent qualification in a relevant engineering discipline.

Additional requirements

Applicants should have a very good background in cyber security, policy, vulnerability management and associated standards. A background in cyber security monitoring system design or operation is an asset.
Knowledge of modern computer systems, programming languages, engineering standards and tools such as DOORs is required. Familiarity with development of large space ground segment is desirable along with demonstrated experience in cyber security engineering for large projects.

Applicants must be eligible for security clearance by their national security administration.
They must be willing to travel.

Other information
For behavioural competencies expected from ESA staff in general, please refer to the ESA Competency Framework.

The working languages of the Agency are English and French. A good knowledge of one of these is required. Knowledge of another Member State language would be an asset.
The Agency may require applicants to undergo selection tests.

The closing date for applications is 07 May 2018.

If you require support with your application due to a disability, please email contact.human.resources@esa.int.

Please note that applications are only considered from nationals of one of the following States: Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Sweden, Switzerland, the United Kingdom and Canada and Slovenia and in addition of Member States of the European Union not members of ESA: Bulgaria, Croatia, Cyprus, Latvia, Lithuania, Malta and Slovakia.

According to the ESA Convention the recruitment of staff must take into account an adequate distribution of posts among nationals of the ESA Member States. Priority will first be given to internal

candidates and secondly to external candidates from under-represented Member States when short-listing for interview. (http://esamultimedia.esa.int/docs/careers/NationalityTargets.pdf)

In accordance with the European Space Agency's security procedures and as part of the selection process, successful candidates will be required to undergo basic screening before appointment.