Job Title: GNSS Cyber Internal Auditor

Req ID **4341** - 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
GNSS Cyber Internal Auditor

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

Location
ESTEC, Noordwijk, The Netherlands

Description
GNSS Cyber Internal Auditor in the Navigation Security Office, Directorate of Navigation.

Duties

The postholder will report to the Head of Office in managing the following activities:

- participating in cyber boards comprising the Cyber Security Manager (CSM) and the Cyber Internal Auditor (CIA) of the EC, ESA and GSA, to provide recommendations on decision-making for cyber management, in particular when granting requests for waivers to applicable cyber requirements and cyber policy from the European Commission;
- ensuring correct flow-down and follow-up of cyber requirements and policies defined by the programme at ESA and industry levels for the Galileo and EGNOS infrastructures for development projects under ESA responsibility;
- planning, organising and conducting periodic audits of cyber security at the Galileo and EGNOS infrastructures for development projects under ESA responsibility;
- evaluating the level of compliance of the information security management system and implemented security measures with the applicable cyber requirements and cyber security policies;
- providing independent feedback on the effectiveness and efficiency of the information security management system and security measures;
- carrying out this role impartially and independently of Galileo and EGNOS project management authorities;
- reporting directly to the Director of Navigation any major cyber security issues identified in carrying out these independent auditing tasks;
- maintaining the directorate cyber audit plan and ensuring that any audit requests issued by the Director of Navigation, GSA or European Commission are taken into account;
- reporting regularly (at least every six months) to the Director of Navigation and also directly to the CSM and CIA of the European Commission on the cyber status of infrastructures in development under Directorate responsibility (Galileo first and future generations, EGNOS);
- compiling cyber reports from the CIA appointed by ESA contractor entities in charge of EGNOS and Galileo infrastructure development;
- reporting any cyber incident related to Galileo/EGNOS immediately to either the Galileo and EGNOS CSMs or to the Galileo Security Monitoring Centre (GSMC);
- interfacing when necessary with the ESA Security Office and/or Galileo Security Accreditation Authority (Galileo Security Accreditation Panel, GSAP, Security Accreditation Board, SAB);
- participating (as observer/cyber adviser) in Galileo and EGNOS project reviews related to infrastructure development;
- participating (as observer/cyber adviser) in Galileo and EGNOS acceptance reviews in particular when the cyber status is discussed;
- participating as a permanent member in cyber boards internal to the ESA Navigation perimeter (Galileo, EGNOS) and in mission-level cyber boards (Galileo, EGNOS);
- regular reporting to the Head of Navigation Security Office.

Technical competencies
Cyber security (policy, detection, reaction, correction)
Cyber vulnerability management and associated standards
State-of-the-art knowledge in area of responsibility at required level
Design, development, deployment and testing of complex secure systems
System engineering
Security auditing standards

Behavioural competencies
Communication
Problem Solving
Relationship Management
Results Orientation
Integrity

Education

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

Additional requirements

Applicants should have substantial project phase C/D/E experience, together with solid system engineering experience in design, development, deployment and testing of complex secure systems. They are expected to have a very good background in cyber security, policy, vulnerability management and associated standards. A background in cyber security monitoring is also expected. Candidates are expected to demonstrate excellent management and organisational skills. They must have experience with high-level stakeholder management. They must possess good judgment, integrity and good communications skills, and be willing to travel. Applicants must have security clearance from their national security administration.

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.

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. When short-listing for an interview, priority will first be given to internal candidates and secondly to external candidates from under-represented Member States. (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.

Recruitment will normally be at the first grade in the band (A2); however, if the candidate selected has little or no experience, the position may be filled at A1 level.