

Job Title: Head of the Galileo First Generation System Security Service

Req ID 10163 - Posted 04/09/2020



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

Head of the Galileo First Generation System Security Service

This post is classified A5 on the Coordinated Organisations' salary scale.

Location

ESTEC, Noordwijk, The Netherlands

Description

Under the direct authority of the Head of the Galileo First Generation Project Office, the Head of the First Generation (G1) System Security Service is in charge of security-related activities for Galileo First Generation including end-to-end system security engineering, design and development of Galileo Public Regulated Service (PRS) infrastructure, as well as security accreditation and cyber security. If recruited to this position, you will be accountable vis-à-vis Security Authorities for the good performance of the Galileo system.

Duties

The main duties of the Head of G1 System Security Service are as follows:

- Implementing overall systems security engineering, including security requirements flow-down, implementation follow-up, security operations engineering and maintenance of the System Security Requirements (SSRS) Statement of Compliance (SOC);
- Defining and maintaining the technical (functional, performance, operational) security requirements applicable to procurement of the overall system infrastructure, namely space and ground segments, and associated operations and launcher services, ensuring their overall traceability;
- Supporting the G1 System Engineering Services in the definition of the new Galileo First Generation Navigation services (OS NMA, HAS, CAS, EWS) to ensure their compliance with mission and system security requirements;
- Monitoring the correct implementation of the system security requirements at all levels within the Project ensuring technical end-to-end consistency;
- Supporting the procurement of the security equipment on-board satellites and within the ground segments in coordination with the Galileo Space Segment and Ground Segment Management Offices;
- Contributing to the overall qualification at System and Segment level of the security requirement and to the deployment of the associated space and ground infrastructure in coordination with the Galileo G1 System AIV and Deployment Service;
- Providing G1 Public Regulated Service (PRS) engineering, including requirements definition and concept of operation for navigation performance and access control and the associated PRS qualification tools, including procurement of test user receivers;
- Supporting the implementation of the PRS IOC and FOC Services, including completion of the associated system infrastructure and service milestones as well as the corresponding service validation activities;
- Interfacing with Competent PRS Authorities (CPAs) in the field of PRS receiver development and validation as well as PRS access control with the objective of continuously aligning the development of Galileo infrastructure with PRS user needs and PRS concept of operation.

Duties continued

- Procurement and maintenance/evolution of the Security Chain Test Bench as well as of the PRS Test Bench located in the PRS Laboratory (including TURP and PRS System Test Tools) required for PRS end-to-end system testing;
- Carrying out Cyber Security activities including definition of Cyber Security requirements and implementation policy for Galileo in compliance with EU Cyber Security requirements and approval of cyber deviations and waivers at system level in coordination with the ESA Security Office (ESO) before submission to the Cyber Program Board;
- Performing the System Penetration Tests and Security Audit of the System Core infrastructure;
- Supporting the procurement of the Security Monitoring infrastructure and its deployment and operations service readiness in coordination with the Galileo Space Segment and Ground Segment Management Offices;

- Threatening core infrastructure accreditation (threat scenario coverage, risk treatment plans, risk analysis) supported by the ESA Security Office (ESO) integrated support, in support of overall accreditation activities performed by the GSA;
- Performing preliminary risk analysis in accordance with specific needs of the project and associated with the evolutions of the Galileo core infrastructure and the new Galileo services and follow-up of the implementation of the associated risk treatments at segment and system level;
- Coordinating the overall system documentation as required by the SAB to support the accreditation process;
- Supporting the G1 System Engineering Service (NAV-NFS) in the definition of the FOC Roadmaps and the G1 System AIV and Deployment Service (NAV-NFD) in the definition of the System DDVP and the integrated Project-level schedule and contributing to the overall risk management at the level of the FOC Project Manager;
- Managing at Project level, in coordination with the Head of the Navigation Security Office, the interface with different bodies for Galileo First Generation security aspects (EC, GSA, SAB, GSB, Member States, ESO) in line with the provisions of the different agreements with EC/GSA;
- Interfacing with the Working Group of National Experts Team, the WG-TEC, WG SPECIAL PRS, the Security Accreditation Panel (GSAP) and the Crypto Distribution Authority task force (CDA TF);
- Coordinating with the Head of the G2 System Security Service (NAV-NEX) to ensure consistency between G1 and G2 security activities.

In discharging these duties, you will manage a team of teams in security engineering and will closely coordinate with the G1 System Engineering service, the G1 System AIV and Deployment Service, the Galileo Ground Segment Management Office, and the Galileo Space Segment Management Office. You will also interface with the G1 PA Manager and the Head of the G1 Project Management Support Office.

Technical competencies

Knowledge and Experience in the following security engineering domains: cyber security, security accreditation, cryptographic systems
 Knowledge and Experience in Satellite navigation system and related security architectures
 Knowledge and Experience in the application of satellite navigation with stakeholders from the security domain in Europe
 In-depth experience of managing EU and national security processes, policies and frameworks

Leadership competencies

Driving performance
 Fostering cooperation & effective team-working
 Developing & motivating people

Behavioural competencies

Problem Solving
 Results Orientation
 Planning & Organisation
 Customer Focus

Education

A Master's degree or equivalent qualification in engineering is required.

Additional requirements

You will also be required to:

- manage individuals or a team in a project setting;
- organise their activities and ensure a motivating work environment;
- have strong leadership capabilities, with proven relationship management and communication skills;
- drive your team's performance, developing their people by encouraging learning, delegating responsibility and giving regular and constructive feedback;
- have strong problem-solving skills to deal with day-to-day operational challenges, together with demonstrated planning and organisational skills;
- have a strong results orientation with the ability to set priorities and present practical solutions both orally and in writing;
- manage challenging situations proactively and constructively and to be customer focused.

People management experience is an asset, as is international experience, i.e. outside your home country, as well as experience in diverse functional areas relevant to ESA activities.

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 02 October 2020.

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, Canada, Latvia and Slovenia and in addition of Member States of the European Union not members of ESA: Bulgaria, Croatia, Cyprus, 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. 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.

Candidates shall be eligible for security clearance by their national security administration.