Organisation for Joint Armament Co-operation
Executive Administration

VACANCY NOTICE

Post	AF31 - INFOSEC & COMMUNICATION SYSTEMS COORDINATOR
Nationality	Vacancy is only open to nationals of a MALE RPAS Programme participating State (Germany, France, Italy and Spain).
Grade, Step, Salary	Grade A4, Step 1 We offer an excellent compensation package. Find out more on our remuneration webpage
Division	MALE RPAS Programme Division
Section	Technical Section
Management of Staff	0
Location	Munich/Hallbergmoos, DE
Initial Contract Duration	3 years
Closing Date for Applications	06/06/2025
Start Date	01/09/2025
Interview Date	Week commencing on 30 June 2025

1. Background

The European Medium Altitude Long Endurance (MALE) Remotely Piloted Air System (RPAS) Programme is a multinational cooperative Programme with the participation of the Federal Republic of Germany, the French Republic, the Italian Republic and the Kingdom of Spain.

The MALE RPAS Programme Division (MRPD) is responsible for the execution of the Contracts for the Definition, Development, Production and In Service Support for the MALE RPAS, and of any potential additional Contracts in specific areas, e.g., ATI... against High Level Objectives defined by the PPSs.

The MALE RPAS Programme Division is based in Hallbergmoos (Munich area), Germany.

Over the last years, the MALE RPAS Programme has successfully passed towards gradual key milestones. A Definition Study was launched in 2016 to define common requirements among the Programme Participating States and was successfully concluded in 2018 with the System Preliminary Design Review (SPDR).

The Invitation for Tendering for a Stage 2 Contract (Development and Production including 5 years of Initial In Service Support) was launched in October 2018. The subsequent two years were fully devoted to negotiating and refining the industry offer to ensure that the contract would meet PPS' expectation in terms of performance, affordability and value for money. The BAFO for the Stage 2 Contract received on 18 November 2020 confirmed the necessary conditions, prices and performances are set to launch soon the programme with an aim of Stage 2 Contract signature end 2021, beginning 2022. In 2021, OCCAR received a Grant from the European Commission (100 M€) to co-fund the Programme and supported PPSs in their national staffing of the Stage 2 Contract. The Stage 2 Contract was signed on 24 February 2022. In 2023 the Preliminary Design Review progressed significantly and was completed in May 2024.

In this context, the Technical Section (TS) is responsible for MALE RPAS Programme Division technical matters, including qualification, certification, airworthiness and information security accreditation related activities, by ensuring the implementation of the Stage 2 technical requirements Contract compliance.

2. Duties and Responsibilities

The INFOSEC and Communication Systems Coordinator will report to the Technical Section Leader (TSL) and be responsible for the management of activities covering the CIS Security requirements of the European MALE RPAS. These activities are carried out in close collaboration with Industry and the National Authorities.

In particular, they will:

- Manage the high-level activities, related to "Information Security" (INFOSEC) and the Communication Systems' (COMMS) requirements;
- Provide expertise in Governmental Information and Communications Technology (ICT) Management;
- Manage all aspects regarding the COMMS and INFOSEC qualification matters, in cooperation with the Certification/Qualification staff and in further co-operation with Joint Accreditation Board (JAB);
- Liaise with the National and International organisations, the Prime and associated MSCs, as necessary;
- Support the Certification and Qualification Team Manager (CQTM), the CQC Manager, and the JAB or any of their respective subpanels/Working Groups, as required;
- Monitor and manage the INFOSEC & Communication Systems' risks within the MRPD;
- Report to the TSL on the Contractors' performance against INFOSEC and COMMS documents, deliverables, developments, production and in services activities;
- Liaise and coordinate, as appropriate, all higher level technical aspects of responsibility in any transversal area of INFOSEC and COMMS matters (or any other transverse affected CQ Panels, e.g.: Safety);
- Monitor the COMMS requirements Qualification and Certification activities status, under COMMS CQ Panel responsibility;

- Monitor the INFOSEC requirements Accreditation, Qualification and Certification activities status, under INFOSEC and associated Sub-WGs responsibility;
- Monitor the "specific Certification Plans" progress, as needed;
- Provide periodic updates (as requested) to senior management or to PPSs during formal meetings (e.g.: PWG, PC, etc.);
- In the absence of the INFOSEC or COMMS Technical Officers, assume the responsibilities toward the TSL, as needed;
- Support all relevant meetings preparation and conduct, including JAB sub-panels (COMSEC, TEMPEST and ICP), CISSWG and COMMS panel and act as chairman if directed by the TSL;
- Performs other tasks and duties in support to the TSL or the PM, as required/needed.

3. Key competences and skills required for the grade

(You must provide evidence of meeting these key competences and skills in your Application, Section 12).

CS 1 Executive management skills and the ability to manage complex negotiations as well as dealing with difficult situations such as conflicts proven through results attained in performing jobs in this field for other national/international organisations;

CS 2 Excellent interpersonal, team working and leadership skills with the ability to interact sensitively, effectively and professionally with people from diverse cultural, educational and professional backgrounds;

CS 3 Conceptual thinking with the ability to analyse complex and wide-ranging questions, issues and information, with a structured approach to the problem-solving process, including providing recommended solutions and a proposed way forward;

CS 4 The ability to work in a changing, developing and demanding environment with the ability to orchestrate and implement clear, efficient and logical approaches to work, to manage time, assignments and objectives;

CS 5 The ability to use Computer and Information Technology (ICT) facilities, with a working knowledge of MS Office software.

4. Specialist knowledge and experience required for the post

(You must provide evidence of meeting these specialist requirements in your Application, Sections 10 and 11).

4.1 Essential:

ES 1 Proven experience in Military Aeronautical Communication Systems;

ES 2 Good experience in INFOSEC (incl. implementation of Security Requirements);

ES 3 Proven experience in Systems´ Security Accreditation or Aeronautical Communication systems' Qualification and Certification processes;

ES 4 Good knowledge of NATO Security and Communication Standards;

ES 5 Experience in International Organisations and contractors' interaction.

4.2 Desirable:

DS 1 Experience in Communications Systems integration in military UAV Systems;

DS 2 Previous experience in Security Risk Assessment and Management;

DS 3 Previous Experience in the field of Tactical / Mission communication and C2 Data Links;

DS 4 Good knowledge or experience on CIS Security or COMSEC/TRANSEC or TEMPEST Management, including definition and implementation of cybersecurity requirements evaluation and approval processes.

5. Language Requirements

- ADVANCED level[1] of ENGLISH both oral and written.
- Additional knowledge of another OCCAR Member or Participating State's language will be considered as an asset.

6. Qualifications

A university degree or equivalent qualification with at least 5 years' experience in either:

- Computer Science, or
- Telecommunication, or
- Aeronautical degree specialised in Aerial Comms or Satellite Comms, or
- CIS Security or INFOSEC or CYBERSECURITY.

Any official managing security programs certification such as CISSP, CISM, etc. would be an asset.

[1] The language levels can be found on the OCCAR website, www.occar.int Careers / Applying.

7. Security Clearance

Security clearance at OCCAR Secret level is required for this post - or needs to be obtained within the first 6 months of employment.

8. Applications and Points of Contact

Applicants wishing to apply for this Post should email the completed application and supporting documentation to: application@occar.int

For further information regarding this post please send your inquiry to the same email address.

OCCAR Privacy Statement:

When applying for an OCCAR vacancy, it is necessary for OCCAR to collect and process personal data about you in order to assess and evaluate your suitability for the vacancy, and (if successful) to coordinate with relevant service providers in preparation of your appointment. For further information please visit our web-site: OCCAR Privacy Statement - http://www.occar.int/privacy-data-protection.