Organisation for Joint Armament Co-operation
Executive Administration

VACANCY NOTICE

Post	A914 - INFORMATION SECURITY SPECIALIST 2
Grade	A3
Division	ESSOR Programme Division
Section	-
Management of Staff	0
Location	Bonn, DE
Initial Contract Duration	2 years (starting from the signature of the ProgD)
Closing Date for Applications	16 April 2025
Start Date	01 July 2025 (subject to the signature of the respective ESSOR Programme Decision)
Interview Date	Week commencing on 12 May 2025

1. Background

The aim of the ESSOR Programme is to develop and produce a complete portfolio of European Software Defined Radio (SDR) products to meet the requirement for interoperable tactical communications in multinational deployment of the Participating States, through the following Programme activities:

- Contribute to the development of an autonomous European Defence Technological Industrial Base in SDR through the establishment of the normative referential required for the development and production of a military SDR in Europe;
- Define and maintain a referential system architecture for ESSOR shared at European level and develop an associated certification environment;
- Develop a complete family of SDR applications providing interoperability to tactical communications in the land, 3D, airborne and maritime domain;
- Develop and maintain a through Life Management (TLM) approach ensuring the maximisation of the benefits to the Programme Participating States throughout the entire lifecycle of the developed systems;

- Support the standardisation efforts of the ESSOR products in the relevant for a (e.g., NATO, EDA, Wireless Innovation Forum, FMN).

The tasks carried out within the ESSOR Programme will concern the following activities for the ESSOR Architecture and the HDR waveforms (named as ESSOR Products):

- developing and testing of new waveforms;
- the technical and operational development of the ESSOR Products;
- the standardisation of the ESSOR Products;
- Management of the ESSOR Product lifecycle through functions like ILS, Requirements Management, Information Lifecycle Management, Life-cycle cost estimate;
- Preparation of subsequent Programme stages.

2. Duties and Responsibilities

The Information Security Specialist 2 shall contribute to achieve the technical High-Level Objectives (HLO) of the programme by supporting the Technical Section Leader in the field of information security.

The post holder, as **Information Security Specialist 2**, will:

- be responsible of the general coordination of management activities related to information security;
- coordinate the activities of ESSOR Information Security Working Group (ITSecWG);
- provide regular reports to the Programme Manager as requested;
- maintain, monitor and manage internal and external action lists related to information security;
- draft, coordinate and distributes minutes of ESSOR ITSec Working Group Meetings and other meetings in the field of information security;
- support the Risk Officers in identifying, assessing and mitigate risks related to the information security;
- elaborate common operational exercise scenarios for the ESSOR product also in conjunction to the main multinational exercises (e.g., CWIX);
- support the identification of operational needs and development of a suitable CONOPS for the use of the ESSOR products and their harmonization, especially in the field of the information security;
- review of the contractual deliverables especially the one concerning the security of the ESSOR products;
- conduct and support the security assessment of the ESSOR product capabilities.

The post holder, as **Designated Security Official**, will act under the authority of the Programme Manager and will liaise with Security Section and will:

- support the implementation of internal procedures related to Information Security (IP, OMP, PSI…);
- assist OCCAR Security Section in developing and coordinating approval process for security related documents and procedures (PSI, FSC…);
- establish the Need-to-Know for PD staff for access to classified information and coordinate assessment on the Need-to-Know of visitors to their PD;
- ensure the right management of classified meetings (e.g., use of dedicated meeting facilities, …); and the correct handling, management and transmission of RESTRICTED Information;
- Prepare and distribute to communication partners (Government establishments and industry) relevant Programme-specific encryption keys;
- support and implement programme-specific security arrangements, in particular with regard to aspects of security classification;
- coordinate the process of releasing of classified information to non-Programme Participating States;
- prepare Visit Requests for PD staff members;
- conduct internal and support the external audits related to information security.

If necessary, the post hold will undertake temporary additional tasks:

- for common activities as required, jointly by the Programme Manager;
- for activities concerning only the Participating State from which is a national, as required by the PM.

The post holder shall co-ordinate with the ESSOR Commercial Section, the ESSOR Technical Section and the Programme Manager for all activities.

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 The ability to establish and maintain excellent working relationships at all levels in a multicultural context and with respect for diversity;

CS 2 Excellent interpersonal and team working skills with the ability to interact and communicate at all levels within OCCAR as well as with Nations;

CS 3 The ability to work in a changing, developing and demanding environment;

CS 4 The ability to implement clear, efficient and logical approaches to work, to manage assignments, objectives and time;

CS 5 The ability to use Computer and Information Technology (ICT) facilities and be able to demonstrate a good 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 Knowledge and experience in national security policies and procedures for the protection of classified information of one or more OCCAR Member States and of international organisations;

ES 2 Knowledge and experience in modern encryption standards and techniques;

ES 3 Knowledge and experience in certification (e.g., Common Criteria) and accreditation processes for military communication systems able to manage information up to NATO SECRET;

ES 4 Knowledge and experience in the management and tracking of classified information, up to NATO SECRET, ensuring they are marked, accessed and distributed in compliance with governmental regulation;

ES 5 Knowledge and experience in various military communication systems (e.g., TDL, Ground to Ground, Air to Ground communications), with an understanding of how these systems support military operations and how they must be secured.

4.2 Desirable:

DS 1 Previous working experience on equivalent post within an international organisation;

DS 2 Experience with Cross-Domain Solution, which enable secure information sharing between different classification levels in tactical environments, while ensuring compliance with military regulations;

DS 3 Knowledge and experience in System engineering;

DS 4 Experience in the management of armament programmes in international cooperation;

DS 5 Ability to identify, assess and mitigate risks.

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 in the activities directly related to the described tasks is highly desirable.

7. Security Clearance

Security clearance at OCCAR Secret level is required for this post.

8. Applications and Points of Contact

For further information regarding this Post, please contact:

Serge DEBONO (ESSOR Programme Manager)

Email: serge.debono@occar.int

Applications for this Vacancy Notice should be submitted through the appropriate National Administrations.

Applicants who are **not** Ministry of Defence staff wishing to apply for this Post should email the completed application and supporting documentation to application@occar.int.

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.

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