

**VACANCY NOTICE**

**SECONDED NATIONAL EXPERT TO THE EUROPEAN COMMISSION**

|  |  |
| --- | --- |
| **Post identification:**  (DG-DIR-UNIT) | **DEFIS-C-2\_A** |
| **Head of Unit:**  **Email address:**  **Telephone:**  **Number of available posts:**  **Suggested taking up duty:**  **Suggested initial duration:**  **Place of secondment:** | **Paul Flament**  [**Paul.flament@ec.europa.eu**](mailto:Paul.flament@ec.europa.eu)  **+3222956342**  **1**  **3rd quarter 2022 [[1]](#footnote-1)**  **2 years1**  **☒** **Brussels** □ **Luxemburg** □ **Other: ……………..** |
|  | **☒  With allowances** □  **Cost-free** |
| **This vacancy notice is also open to**  **□    the following EFTA countries :  □ Iceland □ Liechtenstein □ Norway □ Switzerland  □ EFTA-EEA In-Kind agreement (Iceland, Liechtenstein, Norway) □    the following third countries: □    the following intergovernmental organisations:** | |

**1. Nature of the tasks**

Unit C2 is responsible for the management of the GNSS Programmes (Galileo and EGNOS) and is the interface between the stakeholders in the GNSS programmes dealing with the implementation, exploitation and security of Galileo and EGNOS. It therefore deals with the European Space Agency (ESA), the European Union Agency for the Space Programme (EUSPA), the European External Action Service, National Administrations and their Space Agencies, Commission Services and EU Agencies.

Unit C2 is a team of specialists with a technical, security engineering background - and policy experts who are working closely with their counterparts in ESA and the EUSPA on matters related to the technical management follow-up, services and exploitation and security of the programmes.

We propose a position in the Security Team contributing to one or all of the following scope:

1. Contribute to the establishment of Galileo security governance and its maintenance

o Supervise evolution of Programme Security Instructions and associated annexes

o Ensure compliance of procurements and contracts implemented under the Financial Framework Partnership Agreement (FFPA) with EU Space Programme industrial policy provisions

o Analysis of request for waivers from industrial entities and issue the associated recommendations

2. Security of the supply chain

o Ensure monitoring of the supply chain and identification of critical technologies for the EU Space Programme and prepare recommendations for associated procurement policies

o Support impact analysis of industrial transactions in the frame of the Foreign Direct Investment (FDI) Regulation (reference: EU Regulation (EU) n°(UE) 2019/452) ) and contribute to the preparation of formal opinions

3. Cyber Security Policy Implementation

o Assure the function of Galileo Cyber Security Manager, chairing the Programme Cyber Board in charge of assessing waivers to cyber security requirements and issuing the associated recommendations to Commission Galileo Programme Manager for formal acceptance

o Review and approve annual Cyber Audit Plans and reports proposed by ESA and EUSPA. Ensure reporting to Commission Galileo Programme Manager and SAB and propose if necessary recovery actions

o Supervise the implementation and operational commissioning of the Galileo cyber security monitoring system

o Contribute to cyber security implementation in the EGNOS component

4. Crisis Management Plan implementation

o Support the implementation of the Galileo Crisis Management concept and operational procedures in cooperation with the Galileo Security Monitoring Centre (GSMC) operated by EUSPA and the European External Action Service

o Supervise the definition of the Galileo exercise plans under the responsibility of the GSMC and support its preparation in coordination with the stakeholders

o Support the Commission Galileo Crisis Management Cell

5. Contribute to the Commission’s security roles established in the Galileo and EGNOS Space Programme components management plan and security management plans including for ensuring maintenance of the Galileo and EGNOS security baseline, cyber security management and crisis management.

6. Contribute to Galileo operational security management concept definition and implementation by GSA/EUSPA and the relevant stakeholders in compliance with Galileo and EGNOS Space Programme components roadmaps.

7. Contribute to the definition and implementation of the security framework required to ensure Commission responsibilities concerning GALILEO and EGNOS space programme components security management.

8. Support the management of security aspects of EU Space Programme implementation activities led by Commission’s GALILEO and EGNOS unit

The precise scope of the position will be established taking into account the skills of the retained candidate and the needs of the Unit

**2. Main qualifications**

**a) Eligibility criteria**

The following eligibility criteria must be fulfilled by the candidate in order to be seconded to the Commission. Consequently, the candidate who does not fulfil all of these criteria will be automatically eliminated from the selection process.

• Professional experience: at least three years of professional experience in administrative, legal, scientific, technical, advisory or supervisory functions which are equivalent to those of function group AD;

• Seniority: candidates must have at least one year seniority with their employer, that means having worked for an eligible employer as described in Art. 1 of the SNE decision on a permanent or contract basis for at least one year before the secondment;

• Linguistic skills: thorough knowledge of one of the EU languages and a satisfactory knowledge of another EU language to the extent necessary for the performance of the duties. SNE from a third country must produce evidence of a thorough knowledge of one EU language necessary for the performance of his duties.

**b) Selection criteria**

Diploma

- university degree or

- professional training or professional experience of an equivalent level

in the field(s) : space or security engineering, defence, cybersecurity, industrial policy.

Professional experience

* Knowledge and experience in EU security regulation (e.g. crypto devices evaluation and approval scheme) and security management standards (e.g. 27000, 31000 risk analysis methodology, accreditation process, cybersecurity, …)
* Experience in security management in the frame of national programmes
* Knowledge of GALILEO and EGNOS programmes (e.g. EU Space Programme regulation, stakeholders role governance)
* Knowledge of Galileo security baseline (PSI and annexes, SSRS3.9, eSSRS, cyber requirements, etc.) would be an asset
* Experience in team and stakeholder management
* Experience in operations of security systems and incident/crisis management
* Good communication and diplomatic skills.
* The candidate shall be a holder of a Personal Security Clearance issued by the National Security Authority required to access EU Classified Information up to SECRET UE/EU SECRET classification level.

Language(s) necessary for the performance of duties

Excellent spoken and written English.

**3. Submission of applications and selection procedure**

Candidates should send their application according to the **Europass CV format** (<http://europass.cedefop.europa.eu/en/documents/curriculum-vitae>) in English, French or German **only to the Permanent Representation / Diplomatic Mission to the EU of their country**, which will forward it to the competent services of the Commission within the deadline fixed by the latter.The CV must mention the date of birth and the nationality of the candidate. **Not respecting this procedure or deadlines will automatically invalidate the application.**

Candidates are asked not to add any other documents(such as copy of passport, copy of degrees or certificate of professional experience, etc.). If necessary, these will be requested at a later stage.

Candidates will be informed of the follow-up of their application by the unit concerned.

**4. Conditions of the secondment**

The secondment will be governed by the **Commission Decision C(2008)6866 of 12/11/2008** laying down rules on the secondment to the Commission of national experts and national experts in professional training (SNE Decision).

The SNE will remain employed and remunerated by his/her employer during the secondment. He/she will equally remain covered by the national social security system.

Unless for cost-free SNE, allowances may be granted by the Commission to SNE fulfilling the conditions provided for in Art. 17 of the SNE decision.

During the secondment, SNE are subject to confidentiality, loyalty and absence of conflict of interest obligations, as provided for in Art. 6 and 7 of the SNE Decision.

If any document is inexact, incomplete or missing, the application may be cancelled.

Staff posted in a **European Union Delegation** are required to have a security clearance (up to SECRET UE/EU SECRET level according to Commission Decision (EU, Euratom) 2015/444 of 13 March 2015, OJ L 72, 17.03.2015, p. 53).

The selected candidate has the obligation to launch the vetting procedure before getting the secondment confirmation.

**5. Processing of personal data**

The selection, secondment and termination of the secondment of a national expert requires the Commission (the competent services of DG HR, DG BUDG, PMO and the DG concerned) to process personal data concerning the person to be seconded, under the responsibility of the Head of Unit of DG HR.DDG.B4. The data processing is subject to the SNE Decision as well as the Regulation (EU) 2018/1725.

Data is kept by the competent services for 10 years after the secondment (2 years for not selected or not seconded experts).

You have specific rights as a ‘data subject’ under Chapter III (Articles 14-25) of Regulation (EU) 2018/1725, in particular the right to access, rectify or erase your personal data and the right to restrict the processing of your personal data. Where applicable, you also have the right to object to the processing or the right to data portability.

You can exercise your rights by contacting the Data Controller, or in case of conflict the Data Protection Officer. If necessary, you can also address the European Data Protection Supervisor. Their contact information is given below.

**Contact information**

* **The Data Controller**

If you would like to exercise your rights under Regulation (EU) 2018/1725, or if you have comments, questions or concerns, or if you would like to submit a complaint regarding the collection and use of your personal data, please feel free to contact the Data Controller, HR.DDG.B.4, [HR-MAIL-B4@ec.europa.eu](mailto:HR-MAIL-B4@ec.europa.eu).

* **The Data Protection Officer (DPO) of the Commission**

You may contact the Data Protection Officer ([DATA-PROTECTION-OFFICER@ec.europa.eu](mailto:DATA-PROTECTION-OFFICER@ec.europa.eu)) with regard to issues related to the processing of your personal data under Regulation (EU) 2018/1725.

* **The European Data Protection Supervisor (EDPS)**

You have the right to have recourse (i.e. you can lodge a complaint) to the European Data Protection Supervisor ([edps@edps.europa.eu](mailto:edps@edps.europa.eu)) if you consider that your rights under Regulation (EU) 2018/1725 have been infringed as a result of the processing of your personal data by the Data Controller.

To the attention of candidates from third countries: your personal data can be used for necessary checks.

1. These mentions are given on an indicative basis only (Art.4 of the SNE Decision). [↑](#footnote-ref-1)