Ref. Ares(2026)10756243 - 18/11/2026

Vacancy Notice
Seconded National Expert

IT Security Officer - Cyber Security

Managing Directorate, Civilian Operations Headquarters, Division DSG-DEF.MD-CIVOPSHQ.4
Information Technology and Cyber Sector

AD level post – cost-free

Job no. 529262

WE ARE:

The European External Action Service (EEAS) is the European Union's diplomatic service. Since 2011, the EEAS carries out the EU's Common Foreign and Security Policy (CFSP) to promote peace, prosperity, security, and the interests of the EU across the globe. It brings together European civil servants, diplomats from EU Member States, national experts and local staff worldwide.

The EEAS supports the High Representative in the exercise of her mandate to steer the Union's CFSP, including the Common Security and Defence Policy (CSDP), to represent the EU on issues relating to the CFSP and to chair the Foreign Affairs Council. It also supports her as Vice-President of the Commission with regard to her responsibilities within the Commission, including the coordination of other aspects of the EU's external action. The EEAS works in close cooperation with the EU Member States, the General Secretariat of the Council, the services of the Commission and the Secretariat General of the European Parliament.

The EEAS Headquarters are in Brussels. It is also responsible for the management of the network of 145 Union Delegations and Offices worldwide. These Diplomatic Representations play a vital role in representing the EU in the country where they are based, in promoting the values and interests of the EU, and in building networks and partnerships. They are responsible for all policy areas of the relationship between the EU and the host country/organisation.

WE PROPOSE:

The Civilian Operations Headquarters (CivOpsHQ) is the permanent structure supporting the Civilian Operations Commander/Managing Director (MD). The Civilian Operations Commander is the commander at the strategic level of currently 14 civilian CSDP crisis management missions/Initiative and provides strategic guidance and direction to the Heads of Mission. The Civilian Operations Commander reports directly to the High Representative for Foreign Affairs and Security Policy and through her to the Council of the EU. Under the political control and strategic direction of the Political and Security Committee and the overall authority of the High Representative, the Civilian Operations Commander ensures the effective planning and conduct of civilian CSDP crisis management missions, as well as the proper implementation of all mission-related tasks as well as the discharge of the duty of care.

The successful candidate will be attached to Support Division (CivOpsHQ.4) composed currently of 35 experts in the field of Missions support: Digitalisation, CIS, Cybersecurity, Logistics, Procurement, Contracts and Financial aspects of the civilian CSDP Missions. Our job is to provide operational support for about 2.000 staff working within the 14 CSDP Missions/Initiatives operating in crisis countries.

The Cyber Security Officer will be integrated within the dynamic ICT & Cyber Sector of CivOpsHQ.4, with a focus on providing strong cybersecurity governance and monitoring across the civilian CSDP Missions, in particular in the areas of Governance, Risk and Compliance (GRC), supporting cybersecurity incidents investigation and coordination, threats assessments and identification, as well as supporting overall cybersecurity awareness initiatives.

Functions and Duties

Under the authority of the Head of Division, the Seconded National Expert is expected to perform the following tasks:

- To oversee cybersecurity processes and procedures across all civilian CSDP Missions and work towards their harmonisation.
- To determine cybersecurity vulnerabilities and risks by conducting periodic assessments and propose implementing measures or technical guidance.
- To contribute to the development, implementation and maintenance of the cybersecurity framework covering the civilian CSDP Missions, including overseeing the GRC aspects.
- To provide support in the incident management lifecycle, from detection to investigation and lessons learnt, e.g. via IoC and IoA enrichment, detection rules, coordination of mitigation measures to adopt and follow-up.
- To draft security plans for the securitisation of business-critical applications.
- To support Missions in monitoring their infrastructure and that of the CivOpsHQ via the XDR, SIEM solution in use.
- To participate in the overall team effort of increasing cybersecurity awareness across all Missions and CivOpsHQ staff via the creation of e-learning awareness training, phishing campaigns and live training on cybersecurity threats.
- To participate, when required, in EU cybersecurity related events and meetings in order to assure in-house compliancy with EU cybersecurity related policies.
- To monitor appropriate IT Security metrics and provide periodic status reports to hierarchy for the MSP IT Infrastructure in Brussels.
- To research, evaluate, recommend and introduce new IT security tools, techniques, services and technologies to improve and innovate the MSP (the Mission Support Platform) IT Infrastructure in Brussels.
- To design and perform simulated phishing campaign with specific software in order to assess Mission's awareness level.
- To support external providers of IT security services in the operation of monitoring services, analytical tools, incident management capabilities and the provisioning of engineering/operational services and products/solutions.
- To provide expert advice on topics related to cyber-security and network security.
- To research, evaluate, recommend and introduce new IT security tools, services and technologies to improve and innovate the CivOpsHQ IT Infrastructure in Brussels;
- To participate, when required, in EU cybersecurity working groups, events and meetings;
- To dedicate time throughout the year to self-training and upskilling, also via the platform provided in house.
- Undertake any other related task as requested by the Line Manager(s).

Allowances and financial coverage

Seconded National Experts (hereinafter "SNEs") shall be entitled to:

- reimbursement of mission expenses incurred during the secondment;
- accident insurance policy[1], however accident coverage is not extended to family members.
- where applicable[2], standby duty allowance or shiftwork allowance.

[1] European Union and Institutions FWC PMO/2021/OP/0004.
[2] Article 12(4) of the EEAS SNE Decision (Decision HR DEC(2026) 18 of 20 July 2026).

Start date and duration of secondment

The start date of the secondment shall be the first day of service at the place of secondment.

The initial period of secondment may not exceed two years and may be extended successively up to a period not exceeding four years in total. At the request of the relevant Managing Director or equivalent, the Director responsible for Human Resources may authorise, in exceptional cases and in the interest of the service, one or more extensions of the secondment for a maximum of two years at the end of the four-year period. The total duration of the secondment shall in no case exceed six years.

Position available immediately.

Place of secondment

Brussels

LEGAL BASIS:

This vacancy is to be filled in accordance with the Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 20/07/2026 on the rules applicable to National Experts seconded to the European External Action Service – ADMIN(2026) 18

WE ARE LOOKING FOR:

Eligibility criteria

Candidates must:

a) Have the nationality of an EU Member State, unless a derogation is granted by the Director-General for Resource Management for duly justified reasons in the interest of the service. Such a derogation may only be granted for SNEs assigned to posts in Brussels;

b) Be drawn from Member States' public administrations. In exceptional cases, and with prior authorisation by the Director General for Resource Management, the EEAS may agree to the secondment of national experts from non-EU States' public administrations, non-profit organisations (such as research centres or think tanks) or from international organisations;

c) Be in the active service of the employer on a permanent or contract basis;

d) Have a level of education which corresponds to completed university studies of at least three years attested by a diploma, or where justified in the interest of the service, professional training of an equivalent level;

e) Have at least three years' full-time experience of administrative, scientific, technical, advisory or supervisory functions equivalent to those of function group AD as defined in the Staff Regulations of Officials of the European Union (hereinafter the "Staff Regulations");

f) Have the capacity to work in the languages of the CFSP and external relations (English and French) at a level necessary for the performance of their duties;

g) Have a security clearance issued by the national security authority of an EU Member State that is equivalent at least to the EU classified information level required for the published post[3], notwithstanding the authorised delayed submission of such security clearance as per

[3] Ref. Appendix B 'Equivalent of Security Classification' to the Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU) (OJ L 274, 15.10.2013, p. 1). A description of the EU classified information levels is also available under Decision ADMIN(2025) 42 of the Secretary-General of the European External Action Service of 20 November 2025 on Implementing Rules and Procedures for Personnel Security measures for protection of EU Classified Information, and in Annex A I of the Decision ADMIN(2023) 18 of the High Representative of the Union for Foreign Affairs and Security Policy of 19 June 2023 on the security rules of the EEAS (OJ C 263, 26 July 2023, p.16).

Article 6(3) of Decision ADMIN(2025) 42 of the Secretary-General of the European External Action Service of 20 November 2025[4];

h) Not have been seconded to the EEAS during a period of two years preceding the application for the post. When the former secondment lasted less than six years, a new secondment, which does not exceed the unexpired part of the total six-year period, may exceptionally be accepted less than two years after the end of the prior secondment.

Selection criteria:

A. Professional knowledge

Candidates should have at least three years of professional experience in a cybersecurity or IT security specialist role.

Applicants are expected to have the following experience and skills required for the job:

- Experience with and/or good knowledge of modern security tools and products, in particular related to Cloud, vulnerability assessments and Cyber Threat Intelligence. Knowledge of penetration testing practices can be an asset.
- Knowledge of AI driven threats and related cybersecurity risks.
- Knowledge in Web and Cloud security, including good command of network protocols (TCP/IP, DNS, DHCP, etc.), network architecture, and network device configuration.
- Hands-on experience analysing event logs, network data (e.g. Netflow, FPC), and other attack artifacts in support of incident investigations.
- Knowledge of cybersecurity standards and frameworks, e.g. NIST, CIS controls, EBIOS, ISO 27001/27002 and 27005, SOC2, COBIT, etc…
- Experience with security architectures;
- Have a good knowledge of products, services, technologies and commercial actors related to IT/Cybersecurity sector and their possible applications in modern public administrations;
- Have strong drafting and analytical skills combined with sound judgement;
- Have the ability to communicate clearly on complex issues and the capacity to perform with accuracy and in a flexible manner a diversity of tasks in a complex institutional environment;
- Have strong service attitude;
- Be a positive team player,
- Have excellent command of English both written and spoken.

Furthermore:

- Own a recent/valid professional industry certification(s): e.g. one or more of CISSP, GIAC Certification, CISM, CISA, CRISC; OR a combination of postgraduate certificates and certifications such as CompTIA Security+, CEH Certified Ethical Hacker, etc
- Knowledge of penetration testing practices;
- Experience of working in a team in multi-disciplinary and multi-cultural environment;
- Experience in working with or within other EU institutions, military counterpart or other Governmental entities;

will be considered as assets.

[4] Decision ADMIN(2025) 42 of the Secretary-General of the European External Action Service of 20 November 2025 on Implementing Rules and Procedures for Personnel Security measures for protection of EU Classified Information.

B. Skills required

- Have the ability to remain objective in complex scenarios and to display sensitivity and sound judgement;
- Have good organisational skills, the ability to work under pressure and with tight deadlines and to manage multiple tasks and unexpected demands;
- Have good negotiating skills in a multinational environment;
- Have the ability to work professionally as a member of the division, in mixed-composition task forces and working groups, in an interesting but challenging environment.

C. Languages

Thorough knowledge of one EU working language and satisfactory knowledge of another one are required; in practical terms, in order to perform required duties, that means an excellent command of written and spoken English, in particular good report-writing skills; good knowledge of written and spoken French.

D. Personal Qualities

- Maintain the highest standards of personal integrity, impartiality and self-discipline. The expert must exercise the greatest discretion with regard to all facts and information coming to his/her knowledge in the performance of his/her duties;
- Possess dynamic motivated and flexible personality Be able to adapt quickly to new situations and deal with new challenges, including missions in conflict area.

CONDITIONS OF SECONDMENT:

Conflict of interest

The EEAS shall examine whether candidates have any actual or potential conflict of interest or personal interest such as to impair their independence. To that end, candidates shall inform the EEAS of any actual or potential conflict of interest, taking also into account their professional situation and their family circumstances, in particular their own or their family's professional activities or financial interests. In this context, all candidates shall fill with their application a declaration of potential conflict of interest (Annex I).

As a matter of policy, applications by individuals who have dual nationality of which one of a non-EU country, will be considered on a case-by-case basis taking account in particular of the functions attributed to the vacant post.

Personnel Security Clearance (PSC)

The requested level of security clearance for this post is: **SECRET-UE** / **EU-SECRET**. A description of the EU classified information levels is available under Article 2 of Annex A of the Decision ADMIN(2023) 18 on the security rules of the EEAS[5].

The selected candidate should hold a valid PSC issued by the national security authority of an EU Member State that is equivalent at least to the level indicated in the preceding paragraph, for the duration of the secondment to the EEAS.

Accordingly, all candidates shall fill with their application a declaration of possession of a PSC at the appropriate level (Annex II).

[5] OJ C 263, 26 July 2023, p.16.

In exceptional cases, for reasons duly justified by the seconding authority and after approval by the EEAS Security Authority, the required PSC issued by the national security authority of an EU Member State may be submitted no later than 6 months after the start date of the secondment[6].

Please note that the necessary procedure for obtaining a PSC can be initiated on request of the employer only, and not by the individual candidate.

School fees

Costs related to nurseries and after-school centres managed by the early childhood centre of the European Commission or by any other EU institution, as well as transportation costs to school, shall not be covered by the EEAS. Schooling costs related to the enrolment in a European School Type I shall be covered by the EEAS in compliance with the Convention defining the Statute of the European Schools of 21 June 1994[7]. For further information, please contact RM-01-COORDINATION@eeas.europa.eu.

EQUAL OPPORTUNITIES:

The EEAS strives to be a dynamic, respectful and inclusive Service. We value the talent and professional excellence of our staff, and are committed to building an organisation where gender equality and the respect of diversity are core values, as set out in the EEAS Mission Statement and the EEAS Agenda for Diversity and Inclusion. The EEAS is committed to achieving gender balance within its workforce and strives to avoid any form of discrimination during this selection procedure, as per Article 1(d) of the Staff Regulations. We actively welcome applications from all qualified candidates without any discrimination based on any ground. We commit to recruit candidates with the highest standard of ability, efficiency and integrity, carrying out a selection based on merits required for the post and from the broadest possible geographical basis among the EU Member States.

The EEAS is committed to working with people with disabilities in the terms of the Staff Regulations. If, by virtue of your medical condition or special needs, you require reasonable accommodation for a part or the entirety of this selection process, please send us an email to SNE-CSDP@eeas.europa.eu . Your request will be treated in strict confidence and no record will be kept. If a candidate with a disability is selected for a vacant post, the EEAS is committed to providing reasonable accommodation in accordance with Article 1(d)(4) of the Staff Regulations.

All selected candidates are expected to adhere to the Principles of Professional Behaviour of the EEAS, which outline the need for integrity, transparency, respect, professionalism and accountability, and a zero tolerance approach to any form of harassment.

For queries related to the functions and duties please refer to:

Gloria INIESTA ARIAS, Head of Division, +32 2 584 24 85 gloria.iniesta-arias@eeas.europa.eu

For administrative queries related to the selection process, please refer to:

SNE-CSDP@eeas.europa.eu

[6] During such a period, specific measures shall be taken, including but not limited to those described in Article 7 of the Decision ADMIN(2025) 42 of the Secretary-General of the European External Action Service of 20 November 2025 on Implementing Rules and Procedures for Personnel Security measures for protection of EU Classified Information. Until the PSC is issued by the competent authority of the Member State concerned, the selected candidate will not be authorised to access EUCI at the level of CONFIDENTIEL UE/EU CONFIDENTIAL or above, or to participate in any meetings or workflow where EUCI is processed.

[7] Convention defining the statute of the European schools (OJ L 212, 17.8.1994, p. 3–14).

ANNEX I

DECLARATION OF POTENTIAL CONFLICT OF INTEREST TO BE FILLED BY CANDIDATES

The Decision ADMIN(2026) 18 of the High Representative of the Union for Foreign Affairs and Security Policy of 20 July 2026 establishing the rules applicable to National Experts seconded to the EEAS (hereinafter, the 'EEAS SNE Decision') states:

- in Article 2(3): "*The EEAS shall examine whether candidates have any actual or potential conflict of interest or personal interest such as to impair their independence. To that end, candidates, using a dedicated form, shall inform the EEAS of any actual or potential conflict of interest, taking also into account their professional situation and their family circumstances, in particular their own or their family's professional activities or financial interests. On the basis of the assessment conducted, the EEAS may decide not to proceed with the secondment".*

- in Article 8(1)(c): "*During the secondment, the SNE shall immediately inform their line manager if, in the performance of their duties, they become aware of an actual or potential conflict of interest, or are called upon to give a decision on the handling or the outcome of a matter in which, directly or indirectly, they have a personal interest such as to impair their independence, and, in particular, family's professional activities or financial interests".*

It is the candidates' duty to inform through this form the EEAS of any actual or potential conflict of interest regarding their future tasks. They shall be broad in their identification of actual or potential conflict of interests. It is reminded that it will be up to the administration, and not to the candidates themselves, to assess on this basis whether they are sources of conflict of interests and, if applicable, whether they constitute an issue for the secondment.

Title/First Name/Last Name:

……

……

Position applied for:

……

…

Job number:

……

…

Division:

……

…

Candidate status: ☐ Candidate from a Member State ☐ Candidate from a non-EU country ☐ Candidate from an international organisation ☐ Candidate from a non-profit organisation	
Current and former EU/non-EU nationality(ies):	
Current employer:	
Spouse/partner : Name / Family Name Birth Date EU/non-EU nationality(ies):	
Spouse/partner's professional activities:	
Dependents Name / Family Name Birth Date EU/non-EU nationality(ies):	

In your opinion, do you have any personal interest, in particular a family or financial interest, or do you represent any other interests of third parties which could actually or potentially impair your independence in the course of your duties in the specific vacancy at the EEAS and which may thus lead to any actual or potential conflict of interest relevant to that position?

YES ☐ NO ☐
If yes, please detail:

I hereby certify that the information provided in this form is correct and complete and that my curriculum vitae is correct and duly updated.

I understand that any infringement of the above requirements under the EEAS SNE Decision may lead to the withdrawal of a secondment offer or the termination of the secondment.

Date and signature:

PLEASE FILL IN, PRINT, SIGN AND SCAN

To be returned with the application

ANNEX II

DECLARATION OF POSSESSION OF A PERSONNEL SECURITY CLEARANCE (PSC)

Pursuant to point 19 of Annex A I to the EEAS Security Rules[8] and Article 6(1) of the Decision ADMIN(2025) 42 of the Secretary-General of the European External Action Service of 20 November 2025[9], national experts seconded to the EEAS for a position listed under Article 3(1) and (2) of Decision ADMIN(2025) 42 shall have a valid PSC for access to EUCI in the EEAS prior to taking up their assignment.

I, Mr/Ms _____, hereby declare to be in possession, for the duration of my secondment to the EEAS, of a valid PSC issued by the national security authority of an EU Member State that is equivalent at least to the EU level requested for the published post.

YES ☐ NO ☐

If no, please detail:

I hereby certify that the information provided in this form is correct and complete. I understand that any infringement of the above requirements under the EEAS SNE Decision may lead to the withdrawal of a secondment offer or the termination of the secondment. Date and signature:

PLEASE FILL IN, PRINT, SIGN AND SCAN

To be returned <u>with the application</u>

[8] Decision ADMIN(2023) 18 of the High Representative of the Union for Foreign Affairs and Security Policy of 19 June 2023 on the security rules for the European External Action Service.

[9] Decision ADMIN(2025) 42 of the Secretary-General of the European External Action Service of 20 November 2025 on Implementing Rules and Procedures for Personnel Security measures for protection of EU Classified Information.