EUROPEAN EXTERNAL ACTION SERVICE

Annex 1

European Union Advisory Mission Ukraine

EUAM Ukraine

3-2023 Call for Contributions for Visiting Experts

Requirements and Job Descriptions

Organisation:	**European Union Advisory Mission Ukraine**			
Job location:	**As indicated below**			
Employment regime:	**As indicated below**			
Job titles/ vacancy notice:	**Ref.:**	**Name of the post:**	**Location:**	**Availability:**
	Seconded (4)			
	UAVE 34	Visiting Expert Adviser on Cyber Security	Kyiv/Country wide	March 2026
	UAVE 35	Visiting Expert Adviser on Security Operations Centre Design and Cybersecurity Capabilities	Kyiv/Country wide	March 2026
	UAVE 36 UAVE 37	Visiting Expert Adviser on Investigation and Prosecution of Scam Call Centers	Kyiv/Country wide	March 2026
Deadline for applications:	**07/01/2026 at 17:00 (Brussels time)**			
Applications must be submitted to:	**1) You have the nationality of an EU Member State: you must use Goalkeeper to apply:** **a) You are already registered on Goalkeeper AND you have an EU Login:** **https://goalkeeper.eeas.europa.eu/registrar/web** **b) You do not have a Goalkeeper account or an EU Login:** **https://goalkeeper.eeas.europa.eu/registrar/web/DPA/357/details.do** ***Please note:*** *seconded positions are only available for candidates already validated in the database of their Seconding Authority. Please contact your National Seconding Authority for more information on applying for vacant seconded positions.* *We are unable to provide contact details of National Seconding Authorities.*			
Information:	For more information relating to selection and recruitment, please contact the Civilian Operations Headquarters (CivOpsHQ) : **Mr Bruno FERREIRA** **CIVOPSHQ-HR-EUAM UKRAINE@eeas.europa.eu**			

	+32 460 846 242

According to the EEAS Country Threat Assessment (CTA), the current rating of the host country of the Mission is high/critical. Please note that the CTA of the country might change at any point during the call for contribution cycle. It may have an impact on mission members' working conditions, including financial and leave entitlements.

High/Critical Threat Non-Family Mission – EUAM Ukraine bears a High/Critical Threat Non-Family Mission status due to the present threat rating of the mission area as high/critical. As such, international seconded and contracted mission members shall at no time receive visits or be habitually accompanied by any family member in the mission area for the duration of their present tour of duty or contract.

Seconded personnel – For seconded positions, only personnel nominations received through official channels from EU Member States and Invited Third States (Contributing States) will be considered.

The Mission shall cover the Visiting Experts (VE) travel costs to and from the place of deployment and for any duty travel while on deployment.

Contributing States and EU Agencies will bear all personnel-related costs for seconded VE, e.g. salaries and medical coverage (with the exception of the High-Risk insurance), and allowances other than those paid according to the Council documents 7291/09 (10 March 2009) and 9084/13 (30 April 2013).

Due to the non-permanent nature of VE assignments to Missions, specific provisions may apply with regard to their status, entitlements (e.g. leave days), rights and obligations and security.

Tour of duty – The duration of the deployment is indicated in the respective job description, respectively for an initial 3 months with a possible extension for another 3 months, according to the planned schedule.

The Civilian Operations Commander requests that EU Member States propose candidates for the following international expert positions for EUAM Ukraine, according to the requirements and profiles described below:

I. GENERAL CONDITIONS

Citizenship – Candidates must have a citizenship of an EU Member State or of a Contributing Third State.

Integrity – Candidates must maintain the highest standards of personal integrity, impartiality and self-discipline within the Mission. Selected candidates are not allowed to provide or discuss any information or document as a result of access to classified and/or sensitive information relating to the Mission or respective tasks and activities. They shall carry out their duties and act in the interest of the Mission.

Flexibility and adaptability – Candidates must be able to work in arduous conditions with a limited network of support, with unpredictable working hours and a considerable workload. They must have the ability to work professionally as a member of a team, in task forces and working groups with mixed composition (e.g. civilian and military staff) and be able to cope with extended separation from family and usual environment.

Availability – Candidates must be able to undertake any other tasks related with the competencies, responsibilities and functions of the respective position within the Mission, as required by the Head of Mission.

Serious deficiencies in any of these general conditions may result in repatriation/termination of the secondment/contract.

II. REQUIREMENTS

II.A Essential requirements

The following are essential requirements in respect of civilian international experts to the Missions for all job descriptions:

Physical and mental health – Candidates must be physically fit and in good health without any physical or mental problems or substance dependency which may impair operational performance in the Mission and in its Area of Operation. Selected candidates should undergo an extensive medical examination as requested by the seconding authority or the Mission in accordance with "Fit to work clearance" procedure prior to recruitment/deployment to prove that they comply with the requirement.

To ensure duty of care in the CSDP Mission, selected seconded/contracted candidates shall be able to serve the full period of secondment/contract before reaching the normal age of retirement in Contributing States/country of residence.

Education and training – Candidates should have a recognised qualification under the European Qualifications Framework (EQF), or equivalent, at a level specified in the individual job descriptions. Candidates are strongly advised to verify their compliance through the link: https://ec.europa.eu/ploteus/content/descriptors-page.

Knowledge – Candidates should have knowledge of the EU Institutions and Mission Mandate, particularly related to the Common Foreign and Security Policy (CFSP), including the Common Security and Defence Policy (CSDP).

Skills and abilities

Language skills – Candidates must have the understanding, speaking, and writing proficiency in the working languages of the Mission. Certain positions may require higher language skills further specified in the individual job descriptions. The Mission may seek to facilitate language training and where appropriate, specialist language training, for newly recruited mission staff members. Candidates are advised to verify their proficiency through the following link: https://europa.eu/europass/en/common-european-framework-reference.

Communication and interpersonal skills – Candidates must have excellent interpersonal and communication skills, both written and oral.

Organisational skills – Candidates must have excellent organisational skills, with the ability to prioritise work to meet deadlines, and a concern for order and accuracy.

Digital skills – Candidates must have basic digital skills in the competency areas: information and data literacy, communication and collaboration, digital content creation, safety and problem solving. Candidates are advised to verify their proficiency through the following link: https://digital-strategy.ec.europa.eu/en/news/test-your-digital-skills-and-thrive-digital-world.

Driving skills – Candidates must be in possession of a valid – including Mission area – civilian driving licence for motor vehicles (Category B or equivalent). They also must be able to drive any 4-wheel-drive vehicle.

Serious deficiencies in any of these general conditions may result in repatriation/termination of the secondment/contract.

II.B Desirable requirements

Knowledge of the Mission area – Candidates should have a good knowledge of the history, culture, social and political situation of the region and also knowledge of the police, judiciary and governmental structures, as applicable.

Knowledge and experience of Security Sector Reform – Candidates must be acquainted with Security Sector Reform concepts and practices, especially in the Mission area, as applicable.

Training and experience – Candidates should have attended a Civilian Crisis Management Course or equivalent.

Language – Knowledge of local language(s), depending on the job tasks and responsibilities.

Driving licence – Category C driving licence.

III. ESSENTIAL DOCUMENTS AND EQUIPMENT FOR SELECTED CANDIDATES

Passport – Selected candidates must have a biometric passport from their respective national authorities valid for at least six months. If possible, a Service Passport or Diplomatic Passport should be issued.

Visas – Contributing States and selected candidates must ensure that visas are obtained for entry into the Mission area prior to departure from their home country. It is also essential to obtain any transit visas, which may be required for passage through countries on route to the Mission.

Education diploma(s)/certificate(s) and/or professional certificate(s) – Selected international contracted candidates must have and present to the Mission the university diploma or the professional certificate/diploma, depending on the job description, before signing the contract or taking up their duties.

Required Personnel Security Clearance (PSC) or Certificate of Good Conduct – Selected candidates will have to be in possession of the necessary level of a Personnel Security Clearance (PSC) as specified in the respective job descriptions. In case of lack of such requirement in the job description, selected candidates are required to present a valid official document from their respective country's competent national authority confirming the lack of convictions for crimes or offences under common law, not older than 3 months (the so-called ***Certificate of Good Conduct***).

In case of the PSC requirement: seconded experts must provide the original certificate of the national security clearance or a proof of the initiation of the process upon deployment. For contracted experts, the process will be initiated by the Mission upon deployment. Please note that the role of the Mission is limited to initiation of the process and the Mission declines all responsibility regarding its final outcome.

In any case, the final PSC certificate must be presented within 12 months from the deployment. Failing to meet this requirement will result in the termination of the secondment/contract and no extension can be granted. Please note that Heads of Mission, Deputy Heads of Mission and Senior Mission Security Officers must always provide a valid PSC upon their deployment – a proof of initiation of the PSC is not accepted.

In case of the ***Certificate of Good Conduct***, seconded experts must deliver such a certificate to their respective Seconding Authority. Contracted experts must deliver such a certificate to the Mission's Human Resources before their deployment. In case of possession of multiple nationalities, or if a candidate has or had his/her residence in a country, which is not his/her country of origin, a certificate must be issued by every country where the selected candidate has had his/her residence for a period longer than 1 year during the last 5 years preceding the deployment (except if he/she resided there prior to reaching the age of 18 years).

For Contributing Third States selected candidates, an equivalence to access to the required level of EUCI will be delivered on the basis of Security of Information Agreement or Administrative Arrangements with EU or, in their absence, on the basis of the Framework Participation Agreements.

Certificate/booklet of vaccination – Selected candidates must be in possession of a valid certificate/booklet of vaccination showing all vaccinations and immunisations received. They also must be vaccinated according to the required immunisations for the Area of Operation of the Mission.

Medical certificate – Selected candidates should undergo an extensive medical examination and be certified medically fit for Mission duty. A dental examination is also required to certify that no eminent dental issues are foreseen.

For selected contracted candidates, in compliance with "Fit to work clearance procedure", a copy of the result of the medical examinations as well as the fitness to work certificate, for seconded selected candidate, the fitness to work certificate must be sent to the Medical Adviser of the Mission before joining the Mission. Medical data will be handled with confidentiality and in line with EU Charter of Fundamental Rights and the Standard Operating Procedure on the protection of personal data (CivOpsCdr Instruction 12-2018 as amended.)

The Heads of Mission reserve the right to reject the recruitment of any selected candidate that proves to be medically unfit to work in a civilian CSDP Mission.

Personal protection equipment – It is recommended that national authorities provide seconded selected candidates with protection equipment.

Deficiencies in any of the documents requested for a specific position may result in failure of the selection process.

IV. ADDITIONAL INFORMATION

Equal opportunities – The Mission is committed to an equal opportunities policy for all its staff and candidates, promoting gender equality and to preventing discrimination on any grounds. It actively welcomes applications from all qualified candidates from diverse backgrounds and from the broadest possible geographical basis amongst the EU Member States. It aims at a service, which is truly representative of society, where each staff member feels respected, is able to give their best and can develop their full potential.

Gender balance – The EU strives for improved gender balance in CSDP operations in compliance with EU policy and UNSCR 1325 on Women, Peace and Security (WPS). The CivOpsHQ encourages the EU Member States, European Institutions and the European External Action Service to take this into account when putting forward candidates at all levels.

Application form – Applications will be considered only when using the online application form (AF) accessible on the Goalkeeper-Registrar software module, indicating which position(s) the candidate is applying for. Candidates seconded by Contributing Third States will apply using the dedicated application form returned in Word format.

Selection process – Candidates considered to be most suitable will be shortlisted and, if needed, interviewed in Brussels, at the Headquarters of the Mission or by video conference before the final selection is made. If seconded candidates are required to travel to Brussels/Mission Headquarters for interviews, the Contributing States will bear any related costs. Candidates should be selected on the basis of relevant competence and experience, while strict priority shall be given to seconded candidates. Contracted candidates will be selected only on exceptional basis.

Information on the outcome – Contributing States and contracted candidates (applying for seconded/contracted positions) will be informed about the outcome of the selection process after its completion.

Training – The selected candidates should complete Missionwise and e-SAFE modules, which are designed for the delegations or an equivalent course. The modules can be accessed in the following link: https://webgate.ec.europa.eu/eeas/security-e-learnings.

HEAT Training - Candidates must have undergone a certified Hostile Environment Awareness Training (four to five days residential training) no more than five years ago.

Pre-Deployment Training (PDT) – The selected candidates must have undergone Pre-Deployment Training in accordance with the CSDP agreed Training Policy, or a national alternative of the course.

Code of Conduct – As part of the PDT, the selected candidates must complete the session about the Code of Conduct and Disciplinary Procedure for civilian EU CSDP Missions, also complete the e-learning module on the Code of Conduct prior to their deployment and provide the mission with the course certificate which is kept in their personal file.

Data protection – The EEAS, and its Directorate CivOpsHQ, processes personal data pursuant to Regulation (EC) 2018/1725 on the protection of individuals with regard to the processing of personal data by the EU institutions, bodies, offices and agencies and on the free movement of such data. The Privacy Statement is available on the EEAS website.

V. JOB DESCRIPTIONS

The current reporting lines of the following job descriptions might be subject to modification based on operational requirements and in line with the principles set out in the Operational Plan (OPLAN).

VISITING EXPERT POSITIONS

Position Name: Visiting Expert Adviser on Cyber Security	**Employment Regime:** Seconded	
Ref. Number: UAVE 34	**Location:** Kyiv/Countrywide	**Availability:** March 2026
Component/Department/Unit: Operations Department/Organised Crime and Criminal Justice Component/Organised Crime Unit	**Security Clearance Level:** NOT REQUIRED	**Open to Contributing Third States:** No

1. Reporting Line

The Visiting Expert Adviser on Cyber Security reports to the Head of Organised Crime Unit.

2. Main Tasks and Responsibilities

- To operationalise the Mission mandate and tasks as set out in the planning documents and the Mission Implementation Plan by advising and mentoring local counterparts on the strategic and operational level;
- To support the Mission to address areas of structural weaknesses in the performance and accountability of counterparts/institutions and propose relevant solutions;
- To provide analysis and recommendations to the local counterpart in the area of responsibility;
- To be embedded within the local institution, security permitting;
- To ensure timely reporting on activities as per planning documents;
- To maintain necessary contacts and build relationships with relevant local counterparts;
- To liaise closely with other Mission horizontal advisers;
- To design and deliver training;
- To support the development of the local institutions - National Cyber Security Coordination Centre (NCSCC), State Service of Special Communication and Information Protection (SSSCIP) - in the field of cybersecurity through advisory and capacity building activities as regards prevention, resolution and response to cyber incidents, including establishment of the Security Operations Centre;
- To be the key interlocutor with the NCSCC and SSSCIP and their regional units;
- To develop policies in support of the respective local institutions .
- To support relevant authorities in updating and defining equipment needs (hardware and software, incl. definition of specifications and certification requirements).

3. General Tasks and Responsibilities

- To identify and report on lessons learned and best practices within the respective area of responsibility;
- To contribute and ensure timely reporting on activities within the respective area of responsibility;
- To take account of gender equality and human rights aspects in the execution of tasks;
- To undertake any other related tasks as requested by the Line Manager(s).

4. Essential Qualifications and Experience

- Successful completion of university studies of at least 3 years attested by a diploma OR a qualification in the National Qualifications Framework which is equivalent to level 6 in the European Qualifications Framework OR a qualification of the first cycle under the framework of qualifications of the European Higher Education Area, e.g. Bachelor's Degree OR equivalent and attested police and/or military education or training or an

award of an equivalent rank; AND
- Minimum 5 years of relevant cyber security experience, after having fulfilled the education requirements.

5. Essential Knowledge, Skills and Abilities
- Knowledge of cybersecurity best practices and frameworks' implementation;
- Ability to mentor, advise and motivate local counterparts;
- Experience of designing and delivering training.

6. Desirable Qualifications and Experience
- Experience in international security standards e.g. ISO27000 series or similar;
- International recognised certification(s), e.g. CISM, CISA CISSP, or similar;
- Experience in implementing cybersecurity-related risk management, organisational compliance, auditing and certification;
- Experience in assessing critical entities under the EU Network & Information Security Directive (NIS2) and Critical Entities Resilience Directive (CER), and developing cyber security-related regulatory instructions and guidelines;
- Experience in threat monitoring, incident response, forensic analysis and use of Cyber Threat Intelligence (CTI) platforms and tools;
- International experience, particularly in crisis areas with multi-national and international organisations.

7. Desirable Knowledge, Skills and Abilities
- Ability to build a cybersecurity risk-aware environment and ensure the senior management approves the cybersecurity risks of the organisation;
- Excellent interpersonal and teamwork skills;
- Organisational, analytical and administrative skills;
- Knowledge of Ukraine and/or Russian.

Position Name: Visiting Expert Adviser on Security Operations Centre Design and Cybersecurity Capabilities	**Employment Regime:** Seconded	
Ref. Number: UAVE 35	**Location:** Kyiv/Countrywide	**Availability:** March 2026
Component/Department/Unit: Operations Department/Organised Crime and Criminal Justice Component/	**Security Clearance Level:** NOT REQUIRED	**Open to Contributing Third States:** No

1. Reporting Line

The Visiting Expert Adviser on Security Operations Centre Design and Cybersecurity Capabilities reports to the Head of Organised Crime and Criminal Justice Component

2. Main Tasks and Responsibilities

- To operationalise the Mission mandate and tasks as set out in the planning documents and the Mission Implementation Plan by advising and mentoring local counterparts on the strategic and operational level;
- To support the Mission to address areas of structural weaknesses in the performance and accountability of counterparts/institutions and propose relevant solutions;
- To provide analysis and recommendations to the local counterpart in the area of responsibility;
- To be embedded within the local institution, security permitting;
- To ensure timely reporting on activities as per planning documents;
- To maintain necessary contacts and build relationships with relevant local counterparts;
- To liaise closely with other Mission horizontal advisers;
- To design and deliver training;
- To support the development of the local institutions - National Cyber Security Coordination Centre (NCSCC) and State Service of Special Communication and Information Protection (SSSCIP) - in the field of cybersecurity through advisory activities regarding designing the Security Operations Centre;
- To be the key interlocutor with the NCSCC, SSSCIP and their regional units;
- To develop policies in support of the respective local institutions;
- To provide Engineering Architecture, High-Level Design (HLD) focused on the big picture architecture, defining the system's main components, their interactions, and overall structure, and LLD-Low-Level Design on specific implementation in direct coordination with the beneficiaries' experts;
- To assess, identify and evaluate the gaps in the current cybersecurity crisis management legislative framework, with a focus on information exchange at national and EU MS level, in close coordination with the relevant EUAM advisers and neighboring counterparts from Romania and Moldova.

3. General Tasks and Responsibilities

- To identify and report on lessons learned and good practices within the respective area of responsibility;
- To contribute and ensure timely reporting on activities within the respective

area of responsibility;
- To take account of gender equality, human rights aspects and the human rights-based approach in the execution of tasks;
- To undertake any other tasks as requested by the Line Manager.

4. Essential Qualifications and Experience

- Successful completion of university studies of at least 3 years attested by a diploma OR a qualification in the National Qualifications Framework which is equivalent to level 6 in the European Qualifications Framework OR a qualification of the first cycle under the framework of qualifications of the European Higher Education Area, e.g. Bachelor's Degree OR equivalent and attested police and/or military education or training or an award of an equivalent rank; AND
- Minimum 5 years of relevant professional experience, after having fulfilled the education requirements.

5. Essential Knowledge, Skills and Abilities

- Ability to mentor, advise and motivate local counterparts;
- Experience of designing and delivering training;
- Knowledge of designing and advising and/or professional experience on the national security and cybersecurity crisis management architecture at a strategic level;
- Good knowledge of processes related to establishing situational awareness at national level, EU cybersecurity good practices, and technical solutions;

6. Desirable Qualifications and Experience

- Experience in drafting analytical reports and strategic recommendations;
- International experience, particularly in crisis areas with multi-national and international organisations.

7. Desirable Knowledge, Skills and Abilities

- Excellent interpersonal and teamwork skills;
- Knowledge of the political situation of Ukraine and the threats to the national security;
- Knowledge of Ukraine or/and Russian

Position Name: Visiting Expert Adviser on Investigation and Prosecution of Scam Call Centres.	**Employment Regime:** Seconded	
Ref. Number: UAVE 36 UAVE 37 (2 positions)	**Location:** Kyiv/Countrywide	**Availability:** March 2026 March 2026
Component/Department/Unit: Operations Department/Organised Crime and Criminal Justice Component/Organised Crime Unit	**Security Clearance Level:** NOT REQUIRED	**Open to Contributing Third States:** No

1. Reporting Line

The Visiting Expert Adviser on Investigation and Prosecution of Scam Call Centres reports to the Head of the Organised Crime Unit.

2. Main Tasks and Responsibilities

- To operationalise the Mission mandate and tasks as set out in the planning documents and the Mission Implementation Plan by advising and mentoring local counterparts on the strategic and operational level;
- To support the Mission to address areas of structural weaknesses in the performance and accountability of counterparts/institutions and propose relevant solutions;
- To provide analysis and recommendations to the local counterpart in the area of responsibility;
- To be embedded within the local institution, security permitting;
- To ensure timely reporting on activities as per planning documents;
- To maintain necessary contacts and build relationships with relevant local counterparts;
- To liaise closely with other Mission horizontal advisers;
- To design and deliver training;
- To support the development of the local institutions (the Ministry of Internal Affairs (MoIA), the National Police of Ukraine (NPU), the Office of the Prosecutor General (OPG), the Economic Security Bureau of Ukraine (ESBU), the Security Service of Ukraine (SSU) and the State Financial Monitoring Service of Ukraine (SFMSU) in the field of Transnational Fraud Investigations and Prosecution of Scam Call Centres through advisory support and capacity-building activities;
- To be the key interlocutor with the MoIA and OPG;
- To develop policies in support of the local institutions, particularly MoIA and OPG
- To strengthen the investigative and prosecutorial capacities of Ukrainian law enforcement and prosecutorial authorities in combating scam call center operations and related financial and cyber-enabled crimes through the development of standard operating procedures (SOPs), training, and institutional cooperation frameworks.
- To promote international and interagency cooperation, share EU best practices, and support the establishment of joint investigative and prosecutorial mechanisms with Europol, Eurojust, and EU member states.

3. General Tasks and Responsibilities

- To identify and report on lessons learned and best practices within the respective area of responsibility;
- To contribute and ensure timely reporting on activities within the respective area of responsibility;
- To take account of gender equality and human rights aspects in the

execution of tasks;
- To undertake any other related tasks as requested by the Line Manager(s).

4. Essential Qualifications and Experience

- Successful completion of university studies of at least 3 years attested by a diploma OR a qualification in the National Qualifications Framework which is equivalent to level 6 in the European Qualifications Framework OR a qualification of the first cycle under the framework of qualifications of the European Higher Education Area, e.g. Bachelor's Degree OR equivalent and attested police and/or military education or training or an award of an equivalent rank; AND
- Minimum 5 years of relevant organised crime experience, after having fulfilled the education requirements.

5. Essential Knowledge, Skills and Abilities

- Knowledge of fraud investigation techniques, telecom-based and online scam operations.
- Ability to mentor, advise and motivate local counterparts;
- Experience of designing and delivering training;

6. Desirable Qualifications and Experience

- Familiarity with international cooperation mechanisms such as Europol, INTERPOL, Eurojust, and Mutual Legal Assistance.
- Experience in asset tracing, freezing, and confiscation in fraud-related cases.
- Knowledge of telecommunication and digital payment systems exploited in scam call centre operations and the use of financial or open-sourse intelligence tools.
- Experience in designing or implementing capacity-building initiatives and a sound understanding of EU standards and best practices in combating organised crime and financial fraud.
- International experience, particularly in crisis areas with multinational and international organisations.

7. Desirable Knowledge, Skills and Abilities

- Demonstrated ability to promote an intelligence-led and risk-aware approach within law enforcement and prosecutorial institutions, and effective coordination in countering scam call center operations.
- Proven capacity to interpret and apply international legal frameworks, including mutual legal assistance, data protection, and asset recovery instruments, in alignment with Ukrainian legislation and EU standards.
- Excellent interpersonal, teamwork, organizational, and analytical skills and ability to operate effectively in a multidisciplinary and multicultural environment.
- Knowledge of Ukraine and/or Russian.